# Acano solution 1.6

## Single Combined Acano server Deployment Guide

May 2015

76-1054-01-H

# Contents

## Figures

# 1 Introduction

**Note**: This version of the Deployment guide has a number of sections related to certificates removed and therefore has been slightly reorganized. The information is now in a new Certificates Guidelines document for the single combined solution. See section 1.1.

This guide covers the Acano solution deployed as a single combined server deployment (see the figure below). This deployment has no scalability or resilience.

The server can be an Acano X3 or X2 server, or be hosted on a virtual host (VM); the term "Acano server" in this document covers both.

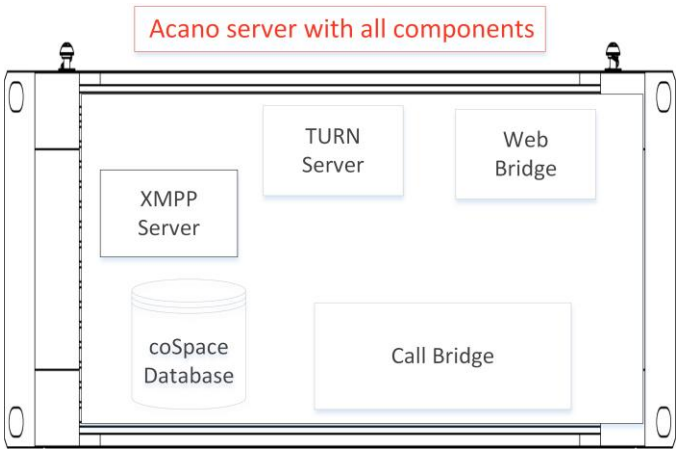



**Figure 1: Single combined server Acano solution deployment**

## 1.1 How to Use this Guide

This guide follows on from the appropriate Installation Guide (see the figure below)—and assumes that you have completed the instructions there already.

Between versions 76-1054-01-C and 76-1054-01-D information on certificates has been removed from this guide and moved to a new Certificate Guidelines document for the single combined solution. For example, the previous appendix C and D have been moved to the new guide and within the body of this document, sections about certificates have been reduced to a single step with a reference to the new document. In addition the guide has been restructured so that all configuration information relating to each component (for example Web Bridge) has been consolidated. This provides one place for all certificate information, another for the configuration relating to each component and reduces duplication.

This deployment guide is intended to be read and acted upon in the order provided. In addition to this guide and the associated Certificate Guidelines, other reference material shown in the figure below can be found at the Acano Documentation & software page. If you need any technical assistance with the configuration, or you want to report a suspected bug, email support@acano.com.

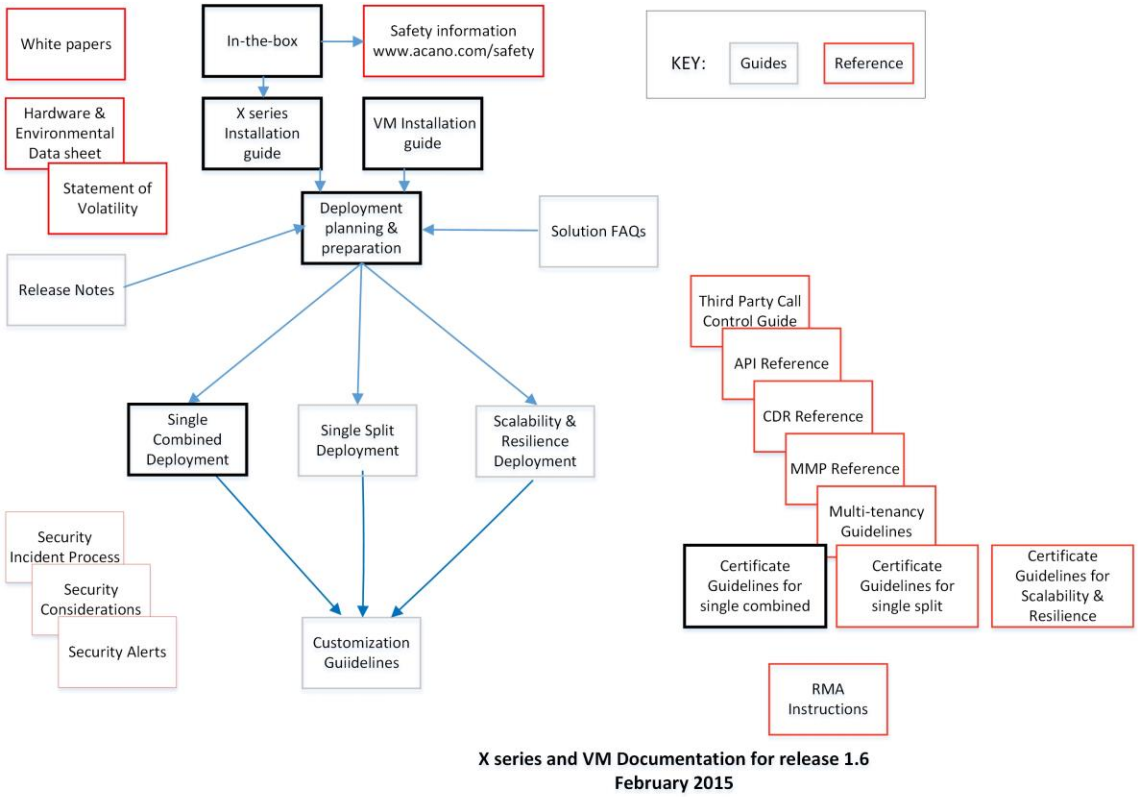



**Figure 2: Installation and deployment documentation**

### 1.1.1 Commands

In this document, commands are shown in black and must be entered as given—replacing any parameters in <> brackets with your appropriate values. Examples are shown in **blue** and must be adapted to your deployment.

### 1.1.2 Management and network interfaces

There are two layers to the Acano solution: a Platform and an Application.

- The Platform is configured through the Mainboard Management Processor (MMP). The MMP is used for low level bootstrapping and configuration. It presents a command line interface.

  Note: On the Acano X series servers the MMP can be accessed via the serial Console port or using SSH on the Ethernet interface labeled Admin. In the virtualized deployment the MMP is accessed on virtual interface A.

- The Application runs on this managed platform with configuration interfaces of its own. The application level administration (call and media management) is done via the Call Bridge's Web Admin Interface which can be configured to run on any one of the Ethernet interfaces.

  On the Acano X series servers there are five physical Ethernet interfaces labeled Admin, A, B C and D. In the virtualized deployment one Ethernet interface (A) is created but up to three more can be added (B, C and D).

Note: There is no physical separation between the media interfaces A-D on an X series server but the Admin interface is physically separate. Each interface is configured independently of the others at the IP level. IP forwarding is not enabled in either the Admin or host IP stack.

See the appropriate (Acano X series or virtualized deployment) Installation Guide for details.

## 1.2 Application Programming Interface

The Acano solution supports an Application Programming Interface (API). The API uses HTTPS as a transport mechanism and is designed to be scalable in order to manage the potentially very large numbers of active calls and coSpaces available in the Acano solution.

The API includes LDAP server access methods for adding, configuring and modifying LDAP servers and support for multi-tenancy for searching calls through an additional Tenant ID. Other additions include posting to coSpace message boards, the ability to filter the set of active call legs to just those experiencing "alarm" conditions (for example, packet loss or excessive jitter) and the ability to retrieve system-wide status values.

Multi-tenancy means that groups of users can be entirely segmented within the solution as required by service provider deployments e.g. users will only be able to meet, assign users to coSpaces, and search in the directory within the same configured customer groups.

Refer to the Acano API Reference guide for more details.

# 2 Prerequisites and Deployment Overview

## 2.1 Prerequisites

The list of items you need prior to installing and configuring the Acano solution in a typical customer environment is given below; some of these items can be configured beforehand:

### 2.1.1 DNS configuration

The Acano solution needs a number of DNS SRV and A records. See this Appendix for a full list but specific records are also mentioned elsewhere.

### 2.1.2 Security certificates

You will need to generate and install X.509 certificates and keys for Acano services which use TLS: Call Bridge, Web Admin Interface (the Call Bridge's interface), Web Bridge and the XMPP server.

The new Certificates Guidelines for single combined deployments contains both background information on certificates and instructions, including how to generate self-signed certificates using the Acano solution's MMP commands. These certificates are useful for testing your configuration in the lab. However, in a production environment we **strongly recommend** using certificates signed by a Certificate Authority (CA).

Instructions that were previously in this guide concerning certificates have been removed and replaced by a single step referencing the new guide.

Note: If you self-sign a certificate, you may see a warning message when you use it that the service is untrusted. To avoid these messages re-issue the certificate and have it signed by a trusted CA: this can be an internal CA unless you want public access to this component.

### 2.1.3 Firewall configuration

See the appendix on Ports required for a summary of the firewall changes you may need to make, and the section on Firewall rules

### 2.1.4 Remote Syslog server

Configure the Acano solution to use a remote Syslog server to store the log files because they contain more detailed logging than is available on an Acano server's own internal log page. (These details are valuable when troubleshooting).

Note: The Syslog server uses TCP not UDP.

Follow the instructions below to define a Syslog server.

1. SSH into the MMP and log in.
2. Enter the following command, `syslog server add <server address> [port]`
   Examples:

```
syslog server add syslog01.example.com 514
syslog server add 192.168.3.4 514
```

3. Enable the Syslog server by entering:

   ```
   syslog enable
   ```

4. Optionally, if you want to send the audit log to a Syslog server follow these steps.

   (The audit log facility records configuration changes and significant low-level events. For example, changes made to the dial plan or coSpace configuration via the Web Admin Interface or the API are tracked in this log file, and tagged with the name of the user that made the change. The file is also available via SFTP.)

   a. Create a user with the audit role.

      ```
      user add <username> (admin|crypto|audit|appadmin)
      user add audituser audit
      ```

   b. Log out of the MMP and log back in with the newly created user account.

   c. Enter the command (this command can only be run by a user with the audit role):

      ```
      syslog audit add <servername>
      syslog audit add audit-server.example.org
      ```

---

Note: Normally Syslog files are overwritten in time but you can permanently store system and audit log files using the new `syslog rotate <filename>` and `syslog audit rotate <filename>` commands. See the MMP Command Reference.

---

### 2.1.5 Network Time Protocol Server

Configure a Network Time Protocol (NTP) server to synchronize time between the Acano components:

1. If necessary, SSH into the MMP and log in.
2. To set up an NTP server, type:

   ```
   ntp server add <domain name or IP address of NTP server>
   ```

To find the status of configured NTP servers: type `ntp status`

See the MMP command reference for a full list of `ntp` commands.

### 2.1.6 Call Detail Record Support

The Acano solution generates Call Detail Records (CDRs) internally for key call-related events, such as a new SIP connection arriving at the server, or a call being activated or deactivated. It can be configured to send these CDRs to a remote system to be collected and analyzed. There is no provision for records to be stored on a long-term basis on the Acano solution, nor any way to browse CDRs on the Acano server.

The CDR system can be used in conjunction with the API, with the call ID and call leg IDs values being consistent between the two systems to allow cross referencing of events and diagnostics.

The CDR receiver is defined in the Web Admin Interface; see the Acano solution CDR Guide for more information. If you are using Acano Manager, it **must** be your CDR receiver.

### 2.1.7 Host name

The hostname must be set for the Acano server:

1. If necessary, SSH into the MMP and log in.
2. Type:

   ```
   hostname <name>
   hostname london1
   hostname mybox.example.com
   ```

3. Type:

   ```
   reboot
   ```

Note: A reboot is required after issuing this command.

### 2.1.8 Other requirements

- Read-only access to the LDAP server in order to import users and calling data automatically. Refer to the section on LDAP configuration for more details.
- Decision on a dial plan to use to reach calls hosted on the Call Bridge. The dial plan will depend on your environment; that is whether you are making one or more of the following types of call: Lync, SIP (including voice) or Acano client calls. Instructions for deploying this dial plan are given in this document
- Access to one or more of the following to test the solution: Lync clients, SIP endpoints phones and/or Acano clients as appropriate
- Access to a SIP Call Control platform if you intend to make SIP calls (for example, using Cisco VCS) to make dial plan configuration changes. The changes required are given in this document

  Note: Information on setting up the SIP Trunk to a Cisco Unified Communications Manager (CUCM), the Avaya CM and Polycom DMA has been removed from appendices in this version of the Deployment guide. The information is now in a new Third Party Call Control Guide available on acano.com/support.

  Note: You can use other call control devices not listed in the Third Party Call Control Guide.

- If you intend to integrate with an audio deployment, access to a Voice Call Control device and this device must be attached to a PBX; it is not possible to connect an Acano server directly to a PBX
- If deploying in a Lync environment, access to the Lync Front End (FE) server to make dial plan configuration changes there. The changes required are given in this document

### 2.1.9 Acano X series-specific prerequisites

- A suitable environment: refer to the Hardware/Environmental Data Sheet for the required power and cooling
- Acano X series servers have two power modules, and, in some countries, country-specific power cables are supplied for the AC power supplies. At installation you must connect both

cables to a power supply socket to implement power supply redundancy (or even to separate power supplies), but the server will work with just a single power unit connected

- 2U of rack space if using the rack mounting kit provided; 3U of rack space if installing on a shelf
- A minimum of two Ethernet links:
  - One for the MMP (labeled Admin on the back of Acano X series servers). The speed can be 100M or 1G
  - One for a media interface (there are four labeled A to D). The speed can be 1G or10G

  IP addresses can be configured statically or automatically via DHCP or SLAAC/DHCPv6. Ethernet links will operate at the speed of the network switch; the switch port should be set to auto-negotiate speed. If you are using a speed of 10G be sure to use the appropriate cable.

See the Acano solution X series Server Installation Guide for full details.

### 2.1.10 Virtualized deployment-specific prerequisites

- A qualified host server with some specific resources. See the Acano solution Virtualized Deployment Installation Guide for full details
- XMPP license file. If you have not already done so, contact support@acano.com providing one of the MAC addresses of the interfaces assigned to the VM to obtain an XMPP license

## 2.2 Deployment Overview

This section outlines the steps required to deploy the Acano server (in addition to the prerequisites from the previous section). See the diagram below.

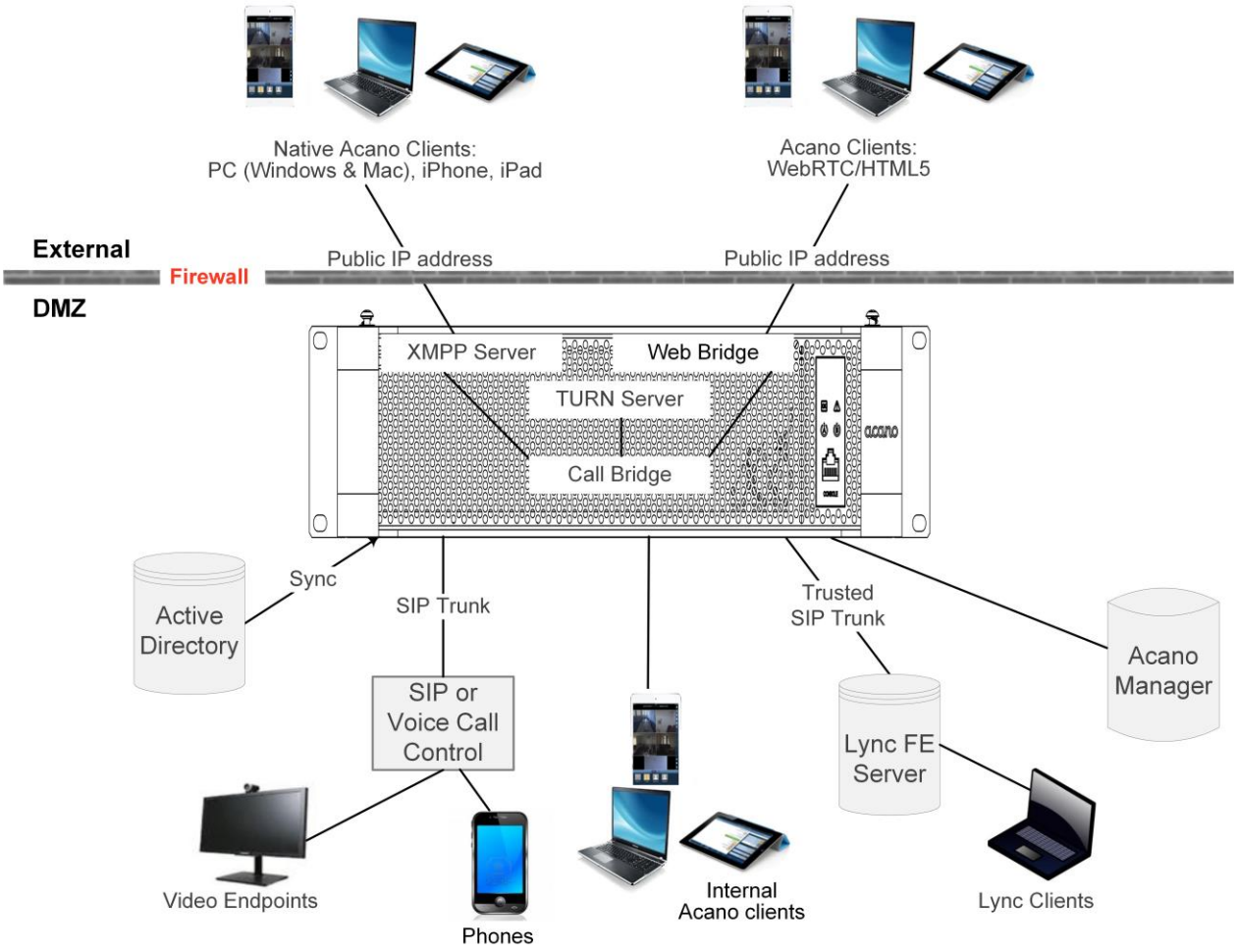



**Figure 3: Example Acano solution using an Acano X series server**

### 2.2.1 SIP trunks and routing

SIP trunks need to be set up to the Acano solution from one or more of the following: SIP Call Control, Voice Call Control and Lync Front End (FE) server. Changes to the call routing configuration on these devices are required to route calls to the Acano solution that require the XMPP service or Web Bridge service for interoperability.

### 2.2.2 Support for Lync clients

You can use both Lync 2010 and 2013 clients connected to a Lync 2010 or 2013 server.

The Acano solution uses:

- the RTV codec transcoding up to 1080p with the 2010 Lync Windows client and 2011 Lync Mac clients
- the RTV codec and H.264 with the 2013 Lync Windows client

Lync 2010 and 2013 clients can share content. The Acano solution transcodes the content from native Lync RDP into the video format used by the other participants in the meeting and sends the content in a separate stream. Lync clients receive content from the meeting in the main video.

The Lync FE Server needs a Trusted SIP Trunk configured to route calls originating from Lync endpoints through to the SIP video endpoints i.e. to route calls with destination in the SIP video endpoint domain through to the Call Bridge.

The SIP Call Control requires configuration changes to route calls destined to the Lync client domain to the Call Bridge so that SIP video endpoints can call Lync clients.

The dial plan routes Lync calls between these two domains in both directions.

The Acano solution includes support for Lync Edge to enable Lync clients outside of your firewall to join coSpaces.

### 2.2.3 Deploying Acano clients

If you are using any of the Acano clients you need to enable the XMPP server, refer to the sections on XMPP Server configuration and Web Admin Interface settings for XMPP. If you are not using the Acano PC Client, iOS Client for iPhone and iPad, Mac or WebRTC Client, disregard all sections referring to the XMPP server.

The following diagram shows example control and media flows during an Acano client call.

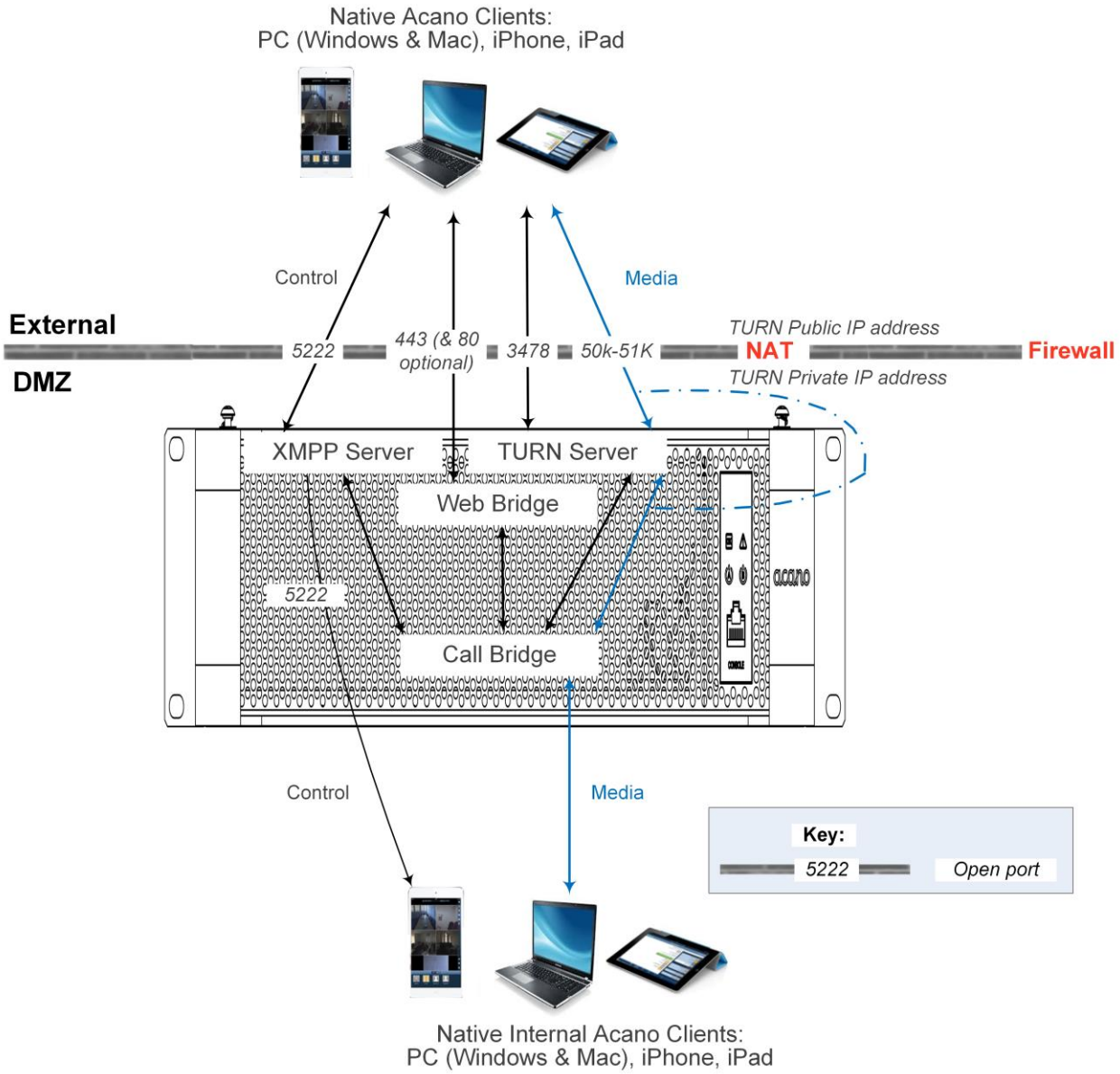



**Figure 4: Example call flow diagram**

Notes on the figure:

Internal clients connect directly to the XMPP server on port 5222 and media connects directly between the Acano client and the Call Bridge.

External Acano clients establish a control connection to the XMPP sever (black line). Media can go directly from the Acano client to the Call Bridge (dashed blue line) or be relayed via the TURN server if required (blue line).

Another deployment option is to enable the XMPP server on a second interface and connect that interface to the private network. Then internal clients can connect directly to the XMPP server. Separate internal and external SRV records for the XMPP service need to be configured, directed to the two interfaces that the XMPP server is listening on.

Both internal and external Acano clients use ICE/TURN to find suitable candidates for connectivity and choose the best: in the case of internal clients this will always be the local host candidates on the internal network.

### 2.2.4 Acano Web Bridge

If you are using the Acano WebRTC Client you will need to enable and configure the Acano Web Bridge, refer to the sections on configuring the Web Bridge and Web Admin Interface settings for Web Bridge. The WebRTC Client works on HTML5-compliant browsers and uses the WebRTC standard for video and audio. For a list of tested devices see the Acano solution Support FAQs.

### 2.2.5 Acano TURN Server

To use Acano clients separated from the Acano solution by a firewall or NAT you need to enable the TURN server, refer to the sections on configuring the TURN server and Web Admin Interface settings for TURN server. The TURN server provides firewall traversal technology.

### 2.2.6 Customization

From R1.6, WebRTC Client customization has changed in some details and additional customization is possible; but some new features require a licence key. See the Acano solution Customization Guidelines for information about the requirements, available features and the specifications e.g. file formats and sizes.

### 2.2.7 Diagnostics and Troubleshooting

In addition to using a Syslog server it is also possible to enable additional SIP tracing using the **Logs > Call Diagnostics** page in the Web Admin Interface. These logs may be useful when investigating call setup failure issues for SIP endpoints and should be disabled at all other times. To prevent the verbose logging being enabled for longer than necessary, it automatically shuts off after a choice of 1 minute, 10 minutes or 30 minutes. Refer to the Acano Support FAQs on the Acano website for more troubleshooting information.

# 3 Configuring the MMP

The Acano solution components are configured using the MMP.

## 3.1 Creating and managing MMP and Web Admin Interface User Accounts

You should have created a MMP administrator user account by following one of the Installation Guides; if so, go on to the next section. The same account is used to access the Web Admin Interface.

(If you do not have an MMP administrator user account, you will have to use the emergency admin recovery procedure detailed in the appropriate Installation Guide.)

Note: To set up additional administrator user accounts and user accounts with other roles and the full range of user commands, see the Acano solution MMP Command Reference.

## 3.2 Upgrading Software

Acano X series servers ship with the latest release available at the time of shipment but may not be up-to-date. Equally, if you downloaded the OVF ZIP file for the virtualized deployment some days ago, we advise you to check on the Acano website whether a later version is available, and if so, upgrade before you start testing. The following instructions apply to both types of deployment:

1. To find out which version the Acano solution is running, SSH into the MMP, sign in and type:
   ```
   version
   ```
2. To upgrade, first download the updated .img file from your Acano reseller.

   NOTE: Ensure that you install the correct image file for your type of deployment; that is either the Acano X series server upgrade file or the virtualized server image file; each is clearly labeled. Note that you may need to rename the file to upgrade.img before going on to step 3.

3. Use a SFTP client to upload a new image to the MMP, for example using a command line SFTP client (where 10.1.x.y is an IP address or domain name):

   For example:

   ```
   sftp admin@10.1.124.10
   put upgrade.img
   ```
4. Then to complete the upgrade, connect via SSH to into the MMP and type:
   ```
   upgrade
   ```
   Allow 10 minutes for the solution to restart.
5. To verify that the upgrade was successful, SSH into the MMP, log in and type the following command to verify that you are now running the version that you intended to:
   ```
   version
   ```

## 3.3 Configuring the Web Admin Interface for HTTPS Access

The Web Admin Interface is the Call Bridge's user interface. You should have set up the certificate for the Web Admin Interface (by following one of the Installation Guides). If you have not, do so now.

1. The port for the Web Admin Interface is 443 **UNLESS** you configured the Web Admin Interface access on the same interface as the Web Bridge. Then set the default TCP port to a non-standard port such as 445 to allow the Web Bridge to function on TCP port 443 with the command
   `webadmin listen admin 445`.
2. To test that you can access the Web Admin Interface, type your equivalent into your web browser: `https://acanoserver.example.com`.

   If it works, proceed to next section.
3. If you cannot reach the Web Admin Interface:
   a. Sign into the MMP, type the following and look at the output:
      `webadmin`

      The last line of the output should say "`webadmin running`".
   b. If it does not there is a configuration problem with your Web Admin Interface. Check that you have enabled it by typing:
      `webadmin enable`
   c. The output of the `webadmin` command should also tell you the names of the certificates you have installed, e.g. webadmin.key and webadmin.crt.

      Note: They should the same names of the certificates you uploaded previously.

      Assuming these are the names then type:
      **`pki match webadmin.key webadmin.crt`**

      This will check that the key and certificate match.
   d. If you are still experiencing issues, troubleshoot the problem as explained in the Certificates guidelines document.

## 3.4 Configuring the Call Bridge

The Call Bridge needs a key and certificate pair that is used to establish TLS connections with SIP Call Control devices and with the Lync Front End (FE) server. If you are using Lync, this certificate will need to be trusted by the Lync FE server.

The command `callbridge listen <interface>` allows you to configure a listening interface (chosen from A, B, C or D). By default the Call Bridge listens on no interfaces; see the MMP Command Reference.

1. Create and upload the certificate as described in the Certificate guidelines document.
2. Sign into the MMP and configure the Call Bridge to listen on interface A.
   **`callbridge listen a`**

Note: Call Bridge must be listening on a network interface that is not NAT'd to another IP address, because Call Bridge is required to convey the same IP that is configured on the interface in SIP messages when talking to a remote site.

3. Configure the Call Bridge to use the certificates by using the following command so that a TLS connection can be established between the Lync FE server and the Call Bridge, for example:

   ```
   callbridge certs callbridge.key callbridge.crt
   ```

   The full command and using a certificate bundle as provided by your CA, is described in the Certificate guidelines document.

4. Restart the Call Bridge interface to apply the changes:

   ```
   callbridge restart
   ```

## 3.5 Configuring the XMPP Server

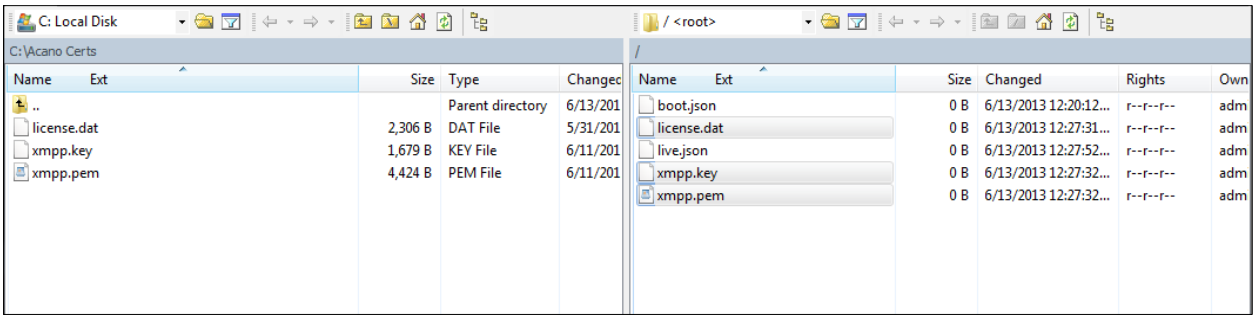
If you are using any of the Acano clients including the WebRTC Client you now need to configure the XMPP server and then enable it. Otherwise, skip this section.

Note: If you had the XMPP server configured before upgrading to R1.6, some of the configuration will be lost on upgrade. Therefore, follow these instructions to ensure that you have a valid configuration.

1. To create DNS A and SRV records for the Acano solution:
   a. Create DNS A record for the fully qualified domain name (FQDN) of the server hosting the XMPP Server and set it to resolve to the IP address of the interface that the XMPP server is listening on
   b. Create DNS SRV record for _xmpp-server._tcp for port 5269 pointing to the DNS A record created in step a above
   c. Create DNS SRV record for _xmpp-client._tcp for port 5222 pointing to the DNS A record created in step a above
   d. Test the above by running the following commands from a PC. They should return the correct IP addresses for these domains:

      ```
      nslookup -querytype=srv _xmpp-server._tcp.example.com
      nslookup -querytype=srv _xmpp-client._tcp.example.com
      ```

2. Sign in to the MMP and generate the private key and certificate using the information in the Certificate guidelines document.
3. On Acano X series servers the XMPP license key file (license.dat) is pre-installed; check it is visible in the list of files. (The example below may look different to your SFTP client). If it is missing contact support@acano.com with the serial number of your X series server.




On a virtualized deployment, you must upload license.dat yourself (using SFTP). If you have not done so already, contact support@acano.com with one of the MAC addresses assigned to the VM to obtain this file. See the Virtualized deployment specific pre-requisites.

The XMPP server can be configured to listen on any subset of the four media interfaces and ignore connections from any interface in the complement.

4. Establish a SSH connection to the MMP and log in.
5. To configure the XMMP server to use one or more interfaces enter the following command:

   `xmpp listen <interface whitelist>`

   The following is an example where interface is set to interface A and B.

   **`xmpp listen a b`**
6. Configure the XMPP server with the following command:

   `xmpp domain <domain name>`

   The following is an example where domain-name is example.com.

   **`xmpp domain example.com`**
7. Enable the XMPP service:

   `xmpp enable`
8. To allow a Call Bridge to access the XMPP server securely (after configuration), provide a component name for the Call Bridge to use to authenticate e.g. example_component:

   `xmpp callbridge add <component name>`

   for example

   **`xmpp callbridge add example_component`**

   A secret is generated; for example, you see:

   ```
   acano>xmpp callbridge add example_component
   Added callbridge: Secret: aB45d98asdf9gabgAb1
   ```
9. Note the domain, component and secret generated in the previous steps because they are required later when you use the Web Admin Interface to configure the Call Bridge access to the XMPP server (so that the Call Bridge will present the authentication details to the XMPP server).

   (If you lose the details, use the MMP `xmpp callbridge list` command to display them.)

## 3.6 Configuring the Web Bridge

The Web Bridge is used by the Acano WebRTC client. If you are testing the WebRTC Client you need to set the network interface for the Web Bridge and then enable it. Otherwise, skip this section.

1. SSH into the MMP.
2. Configure the Web Bridge to listen on the interface(s) of your choice with the following command:

   ```
   webbridge listen <interface[:port] whitelist>
   ```

   The Web Bridge can listen on multiple interfaces, e.g. one on public IP and one on the internal network. (However, it cannot listen on more than one port on the same interface.)

   The following is an example where interfaces are set to interface A and B, both using port 443.

   ```
   webbridge listen a:443 b:443
   ```

3. Create DNS A record for the Web Bridge and set it to resolve to the IP Address of the Ethernet interface you want to use.
4. Create a certificate and private key for the Web Bridge as described in the Certificates guidelines document. Upload the certificate file to the MMP via SFTP.
5. Add the Call Bridge certificate to the Web Bridge trust store as described in the Certificates guidelines document.
6. The Web Bridge supports HTTPS. It will forward HTTP to HTTPS if configured to use “http-redirect”. To do so:
   a. Enable HTTP redirect with the following command:

      ```
      webbridge http-redirect enable
      ```

   b. If required (see the note), set the ClickOnce location and the Windows MSI, Mac OSX DMG and iOS installers that are presented to WebRTC users:

      ```
      webbridge clickonce <url>
      webbridge msi <url>
      webbridge dmg <url>
      webbridge ios <url>
      ```

   Note: If you only use browsers that support WebRTC (e.g. Chrome) you do not need to set these download locations because browser functionality will be used for guest access to coSpaces. However, if you use browsers that do not (e.g. IE, Safari) then configure these locations so that when the Acano solution detects the device being used (iOS device, Mac, or PC), can redirect you to the configured client download link for that device and prompt you to install the correct Acano client so that you can join the meeting. After installation, you are connected to the coSpace as a Guest. (Firefox support is currently in beta.)

7. Enable the Web Bridge with the following command:

   ```
   webbridge enable
   ```

## 3.7 Configuring the TURN Server

1. SSH into the MMP.

2. Configure the TURN server with the following command:

   `turn credentials <username> <password> <realm>`

   The following is an example where username is myusername, the password is mypassword and it uses the realm example.com.

   **`turn credentials myusername mypassword example.com`**

3. If the TURN server located behind a NAT, set the public IP Address that the TURN Server will advertise using:

   `turn public-ip <ip address>`

   Note: If the TURN server has a public IP address rather than being NAT'ed (see the figure below and its notes), this step is not required, go on to step 4.

   The following is an example where a public IP address is set to 5.10.20.99

   **`turn public-ip 5.10.20.99`**

   Note: The IP address set here should not be confused with the IP addresses set in the Web Admin Interface **Configuration > General** page later. The MMP commands configure the TURN server itself, while the **Configuration > General** page settings allow the Call Bridge and external clients to access the TURN server.

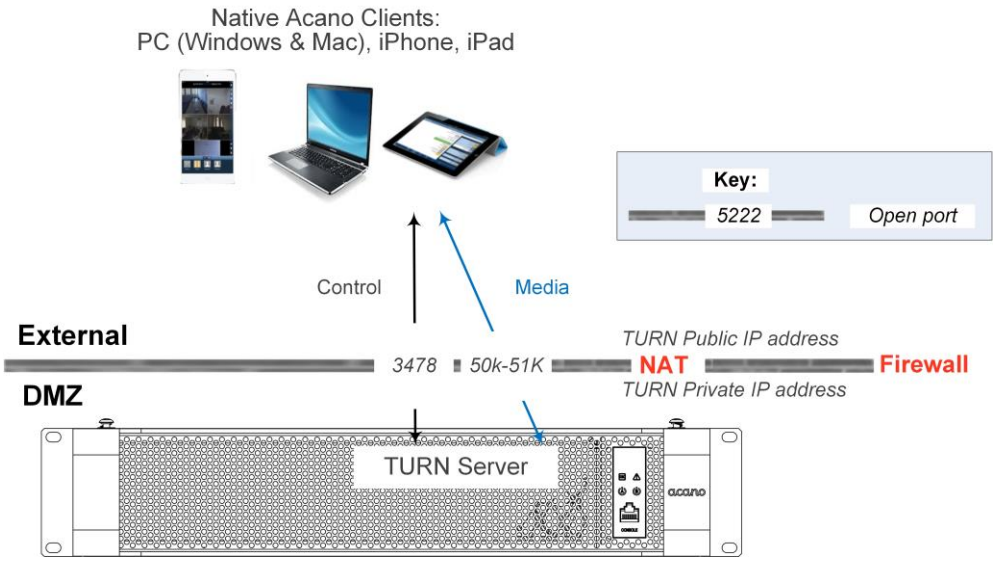



**Figure 5: TURN server public IP address**

4. Configure the TURN Server to listen on a specific interface using:

   `turn listen <interface whitelist>`

   The following is an example where the interface list is set to interface C but you can specific more than one interface

   **`turn listen c`**

5. Enable the TURN server:

```
turn enable
```

# 4 LDAP Configuration

You must have an LDAP server (currently Active Directory or OpenLDAP) to use the Acano solution. User accounts are imported from the LDAP server. You can create user names by importing fields from LDAP. The passwords are not cached on the Acano solution, a call is made to the LDAP server when an Acano client authenticates, and therefore passwords are managed centrally and securely on the LDAP server.

## 4.1 Why use LDAP?

Using LDAP to configure the Acano solution is a powerful and scalable way to set up your environment: defining your organization's calling requirements within the LDAP structure minimizes the amount of configuration required on the Acano solution.

The solution uses the concept of filters, rules and templates.

Filters allow you to separate users into groups, for example:

- Everyone in the HR department
- Staff at grade 11 and above
- Job title = 'director'
- People whose surname starts with 'B'

Then rules (actions) can be applied on these groups, for example:

- Give users in this group the ability to create new coSpaces
- Associate users in this group to one or more existing coSpaces, e.g. the 'HR managers coSpace'
- Create a personal coSpace for each user in this group
- Apply a template to this group of users

Templates define things such as which default layout to use, or what maximum call rate is allowed. For example, if a new employee joins the organization as a manager with a grade >11, just based on his job title or grade he can be set up automatically with a personal coSpace, have the ability to create new coSpaces, have a 4Mbps call rate and be assigned to the "all managers" coSpace. In contrast, another new joiner with job title "temp" might be configured with a default call rate of 500kbps.

Note: Full functionality for LDAP filters and templates will be introduced in a future release.

## 4.2 Acano Solution Settings

Note: The Acano solution supports multiple LDAP servers via the API: the Web Admin Interface only allows you to configure one. See the LDAP Methods section in the API Reference guide.

This example assumes you are using Microsoft Active Directory (AD).

To set up the Acano solution to work with AD, follow these steps:

1. Sign in to the Web Admin Interface and go to **Configuration > Active Directory**.
2. Configure the connection to the LDAP server in the first section with the following:

- Address = this is the IP address of your LDAP server
- Port = usually 636
- Username = the Distinguished Name (DN) of a registered user. You may want to create a user for this purpose
- Password = the password for the user name you are connecting as
- Secure Connection = select this setting for a secure connection

  For Example:

```
Address:  100.133.2.44
Port:     636
Username: cn=Fred Bloggs,cn=Users,OU=Sales,dc=Example,dc=com
Password: password
```

Note: The Acano solution supports secure LDAP. By default the LDAP server runs on port 636 for secure communications and port 389 for insecure communications. The Acano solution supports both but we recommend using 636. Note that you must select Secure Connection (see above) for communications to be secure: using port 636 alone is not enough.

3. The Import Settings control which users should be imported.
   - Base Distinguished Name = the node in the LDAP tree from which to import users. The following is a sensible choice for base DN to import users

     `cn=Users,dc=sales,dc=Example,dc=com`
   - Filter = a filter expression that must be satisfied by the attribute values in a user's LDAP record. The syntax for the Filter field is described in rfc4515.

     A rule for importing people into the main coSpace database might reasonably be 'import anyone with an email address', and this is expressed by the following filter:

     `mail=*`

     For testing purposes you may want to import a named user and a group of test users whose mail address starts with “test”; for example:

     `(|(mail=fred.bloggs*)(mail=test*))`

     If you wanted to import everyone apart from one named user, use this format:

     `(!(mail=fred.bloggs*))`

     To import users that belong to a specific group, you can filter on the `memberOf attribute`. For example

     `memberOf=cn=apac,cn=Users,dc=Example,dc=com`

     This imports both groups and people that are members of the APAC group. To restrict to people, use:

     `(&(memberOf=cn=apac,cn=Users,dc=Example,dc=com)(objectClass=person))`

Using an extensible matching rule (LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941), it is possible to filter on membership of any group in a membership hierarchy (below the specified group); for example:

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=apac,cn=Users,dc=Example
,dc=com)(objectClass=person))
```

Other good examples which you can adapt to your LDAP setup include:

- Filter that adds all Person and User except the ones defined with a !

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))
(!(cn=Guest))(!(cn=krbtgt)))
```

- Filter that adds same as above (minus krbtgt user) and only adds if they have a sAMAccountName

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))
(!(cn=Guest))(sAMAccountName=*))
```

- Filter that adds same as above (Including krbtgt user) and only adds if they have a sAMAccountName

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))
(!(cn=Guest))(!(cn=krbtgt))(sAMAccountName=*))
```

- This filter only imports specified users within (|( tree

```
(&(objectCategory=person)(objectClass=user)(|(cn=accountname)(cn
=anotheraccountname)))
```

- Global Catalog query to import only members of specified security group (signified with =cn=xxxxx

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=groupname,cn=Users,dc=ex
ample,dc=com)(objectClass=person))
```

4. Set up the Field Mapping Expressions

   The field mapping expressions control how the field values in the Acano solution's user records are constructed from those in the corresponding LDAP records. Currently, the following fields are populated in this way:
   - Display Name
   - User name
   - coSpace Name
   - coSpace URI user part (i.e. the URI minus the domain name)
   - coSpace Secondary URI user part (optional alternate URI for coSpace)
   - coSpace call id (unique ID for coSpace for use by WebRTC client guest calls)

   Field mapping expressions can contain a mixture of literal text and LDAP field values, as follows:

   `$<LDAP field name>$`

   As an example, the expression

   **`$sAMAccountName$@example.com`**

   Generates:

   **`fred@example.com`**

For more information see the appendix on LDAP field mappings.

Note: Each imported user must have a unique XMPP user ID (JID), constructed using the JID field in the Field Mapping Expressions section of the **Configuration > Active Directory**. In order to construct a valid JID, any attribute used in the JID field mapping expression must be present in each LDAP record that is to be imported. To ensure that only records that have these attributes present are imported, we recommend that you include presence filters (i.e. those of the form (<attribute name>=*)) using a '&' (AND) in the Filter field under Import Settings for each attribute used in the JID field mapping expression.

For example, suppose your JID field mapping expression is $sAMAccountName$@example.com, and you wish to import users who are members of the group cn=Sales,cn=Users,dc=example,dc=com, an appropriate import filter would be:

```
(&(memberOf=cn=Sales,cn=Users,dc=example,dc=com)(sAMAccountName=*))
```

5. To synchronize with AD, select **Sync now** or activate the synchronization by using the appropriate API call (see the API Specification document).

   Note that you must manually resynchronize whenever entries in the LDAP server change.
6. View the result of the synchronization by going to **Status > Users**.

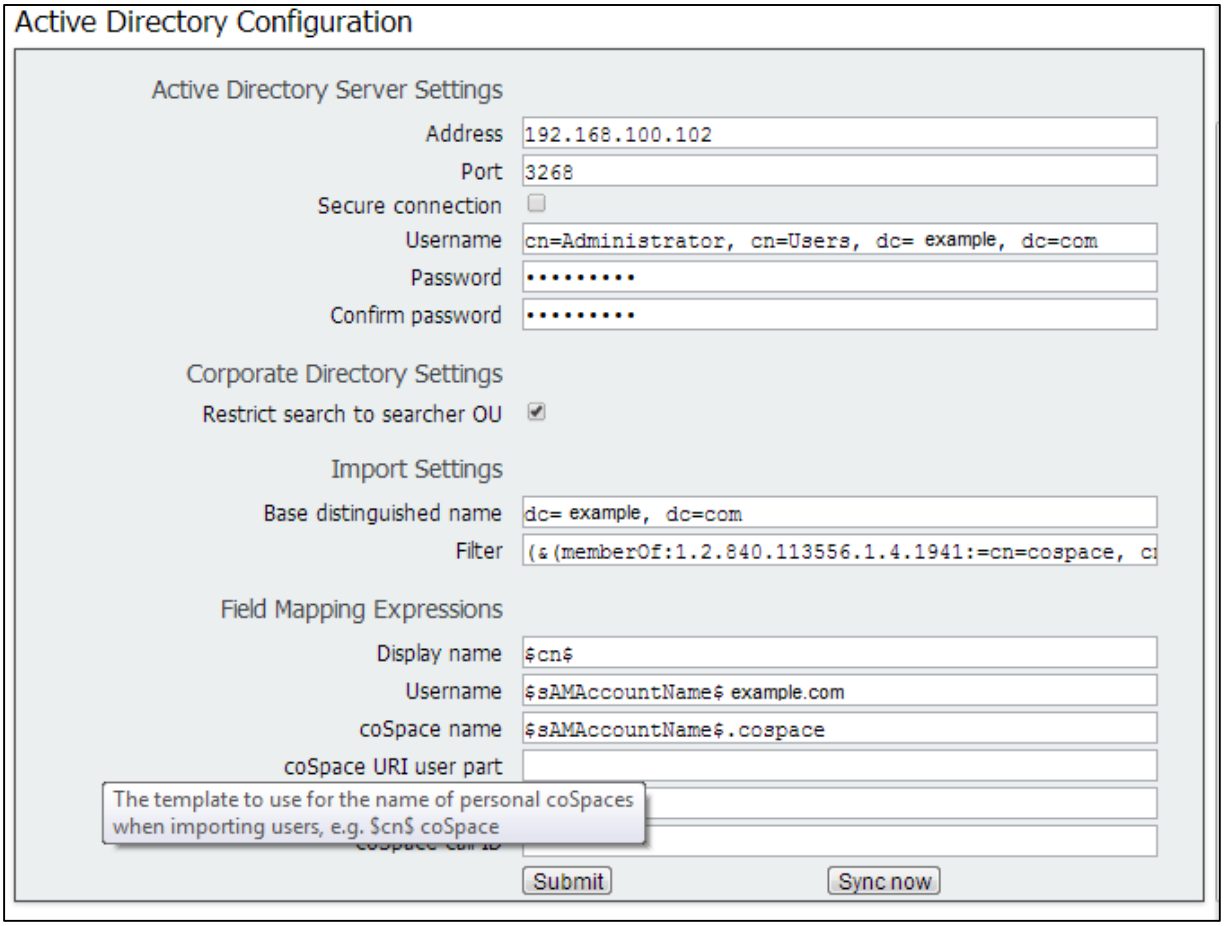
It is possible to choose whether to use OU separation when importing from the LDAP server. In the Web Admin Interface, go to **Configuration > Active Directory** and select Restrict Search to Searcher OU to enable the search only within the OU of the user account.

## 4.3 Example

You want to assign a coSpace to a particular group of users and a Call ID for this coSpace using an 88 prefix in front of the regular telephone number.

1. Create the group on the LDAP structure called "**cospace**" and assign the required members to that group.
2. Use the following filter which uses the extensible matching rule (LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941) to find all the users that are a member of the "cospace" group:

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=cospace,cn=Users,dc=lync,dc=example,dc=com)(objectClass=person))
```




3. Then synchronizing a particular user in the directory called:

   **cn = Fred Blogs**

   **TelePhoneNumber = 7655**

   **sAMAccountName = fred.blogs**

   creates the following coSpace which can be viewed on the **Status > Users** page.

| Name | XMPP id |
|---|---|
| Fred Blogs | fred.blogs@xmpp.example.com |

   And the following coSpace that can be viewed on the **Configuration > coSpace** page.

| Name | URI user part |
|---|---|
| fred.blogs | fred.blogs.cospace |

# 5 Dial Plan Configuration – SIP Endpoints

## 5.1 Introduction

In order for the Acano solution to be integrated in a SIP, Lync and voice environment, connections need to be set up from the SIP Call Control, Voice Call Control and Lync FE server to the Acano solution as shown in Figure 1 above. Changes to the call routing configuration on these devices are required in order to route the calls that require the Acano solution for interoperability correctly to it.

This example (see the figure below) assumes a company deployment which has a mix of SIP video endpoints, Lync clients and IP phones: the Acano solution enables connectivity between Lync clients and SIP video endpoints, and between Lync clients and IP phones.

The SIP video endpoints are configured on a domain called vc.example.com and the Lync clients on example.com. You will need to adapt the example, as appropriate to your existing Lync deployment.

Note: Although this figure and subsequent diagrams in this Deployment Guide use an Acano X series deployment as the example, the instructions apply equally to virtualized deployments.

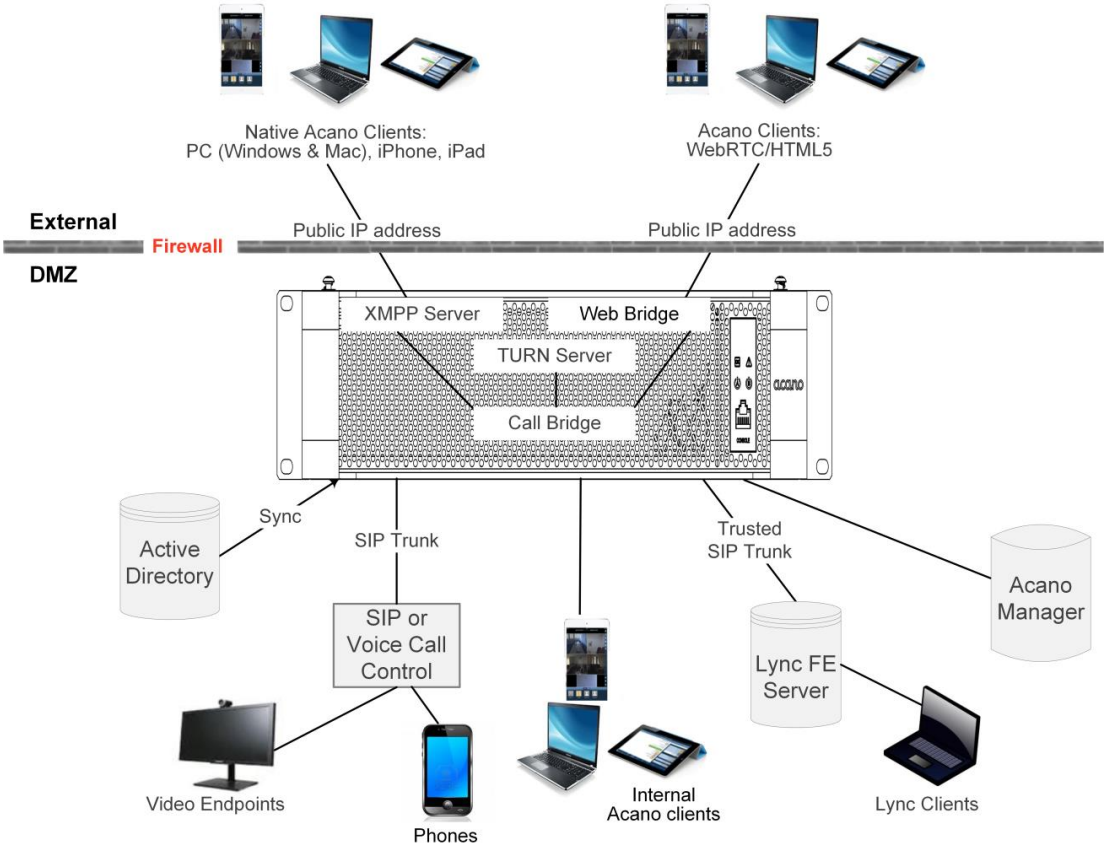



**Figure 6: Example solution for dial plan configuration**

As shown in the figure above, the Lync FE server needs a Trusted SIP Trunk to the Acano solution, configured to route calls originating from Lync clients through to Acano coSpaces, Acano client users (native and WebRTC) and also SIP video endpoints. The subdomains vc.example.com and acano.example.com should be routed through this trunk from the Lync FE server to the Acano solution.

The SIP Call Control platform needs a SIP trunk set up to route calls to the example.com domain (for Lync Clients) and acano.example.com (for coSpaces and Acano clients) to the Acano solution.

The Acano solution requires a dial plan to route calls to example.com to the Lync FE server and vc.example.com to the SIP Call Control platform.

The configuration required for the total solution is built up step-by-step below and therefore, to plan your own installation, work through the steps in the order provided adapting the example as appropriate.

## 5.2 SIP Endpoints Dialing a Call on the Acano Solution

As a starting point, consider using only SIP video endpoints and the configuration on the VCS and Acano server to direct and host calls for these endpoints.

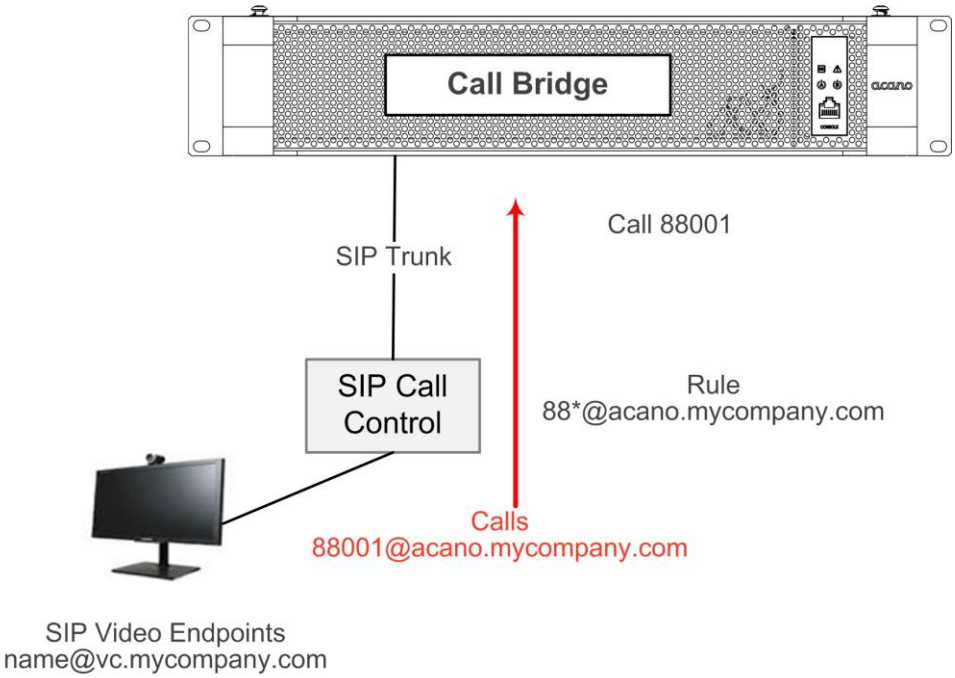



**Figure 7: Example of SIP video endpoints calling into Acano server hosted calls**

### 5.2.1 SIP call control configuration

This example assumes the SIP Call Control is a Cisco VCS but similar steps are required on other Call Control devices. See the Third Party Deployment Guide for other examples such as CUCM and Polycom DMA.

Set up a zone to route calls to the Acano solution by logging into the VCS as an administrator and following the steps below.

1. Go to **VCS Configuration > Zones > New**.
2. Create the zone with the following:
    - H.323 Mode = Off.
    - SIP Mode = On
    - SIP Port = 5060 (5061 if using TLS)
    - SIP Transport = TCP or TLS, as appropriate
    - SIP Accept Proxied Registrations = Allow
    - Authentication Policy = Treat as authenticated
    - SIP Authentication Trust Mode = Off
    - Peer 1 Address = the IP address of the Call Bridge

### 5.2.2 VCS search rule configuration

Add a search rule on the VCS to route calls to the Acano solution by following the steps below (e.g. to route any video endpoint call to a call on the Acano solution using the call prefix 88).

1. Go to **VCS Configuration > Dial Plan > Search rules**.
2. Give the rule a suitable name, e.g. VC EPs to Acano.
3. Set the following:
    - Source = Any
    - Request Must Be Authenticated = No
    - Mode = Alias pattern match
    - Pattern Type = Regex
    - Pattern String = **.*@acano.example.com**
    - Pattern Behavior = Leave
    - On Successful Match = Stop
    - Target = the zone you created for the Acano solution.

### 5.2.3 Creating a coSpace on the Acano solution

Create a coSpace on the Acano solution for endpoints to dial into as follows:

1. Sign in to the Web Admin Interface.
2. Go to **Configuration > CoSpaces**.
3. Add a coSpace with:

- Name e.g. **Call 001**
- URI e.g. **88001**

Note: coSpaces can also be created from the API. See the API Reference guide.

### 5.2.4 Adding a dial plan rule on the Acano solution

1. Still in the Web Admin Interface, go to **Configuration > Outbound Calls** and add a dial plan rule with the following details:
   - Domain = **vc.mycompany.com**
   - SIP Proxy = the IP address or FQDN of your VCS
   - Local Contact Domain =

     Note: The local contact domain field should be left blank unless setting up a trunk to Lync (as in section 6.1.2).
   - Local From Domain = **acano.mycompany.com**
   - Trunk Type=Standard SIP.

SIP video endpoints can now dial into a call 88001 hosted on the Acano solution by dialing 88001@acano.mycompany.com.

## 5.3 Media Encryption for SIP Calls

The Acano solution supports media encryption for SIP connections including Lync calls.

This is configured in the **Configuration > Call settings** page in the Web Admin Interface and allows encryption to be Required, Allowed or Disabled for SIP calls made to or from the Acano solution. Additionally, you can choose whether changes to this setting will apply to SIP calls already in progress (**Apply to Active Calls** button) or just future calls by using the **Submit** button at the end of the **Call Settings** page.

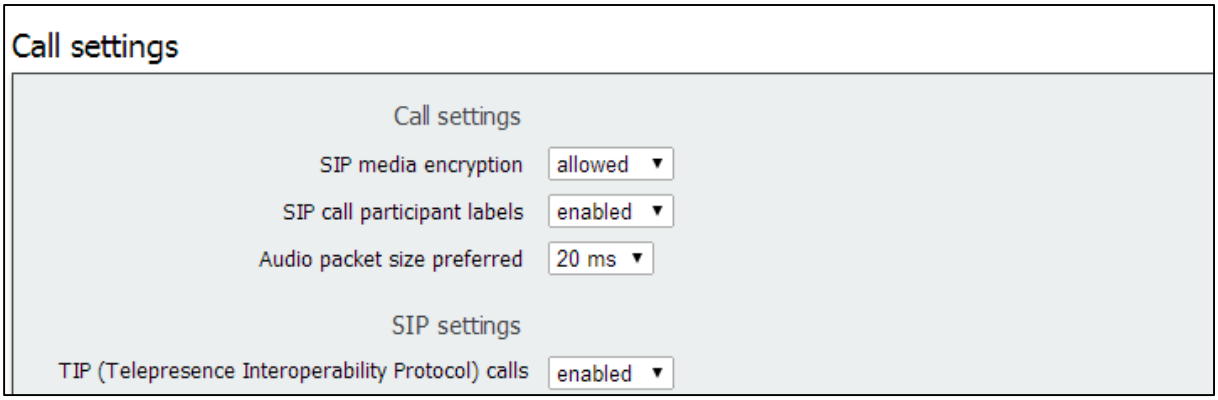
1. Sign in to the Web Admin Interface and go to **Configuration > Call settings.**
2. Select the appropriate SIP Media Encryption setting (Required, Allowed or Disabled).
3. Click either **Submit** or **Apply to Active calls**.

Note: The SIP Encryption field in the Web Admin Interface **Configuration > Outbound Calls** page allows you to set the behavior for each Outbound Calls dial rule. This separates the control and media encryption behavior, allowing a TLS control connection to be used in the absence of media encryption, for example. (You can also control SIP control message behavior via the API (see the API Reference guide.)

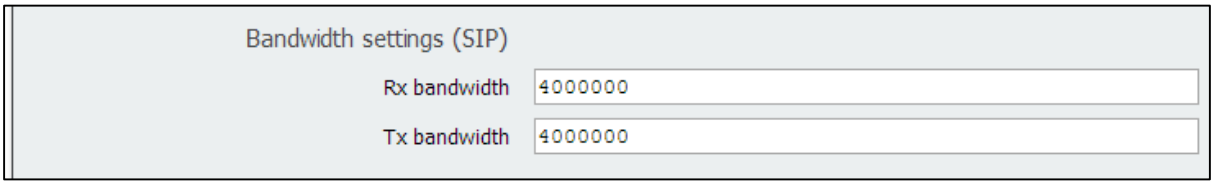
## 5.4 Enabling TIP Support

If you use endpoints such as the cisco CTS range, you require the new TIP protocol support available in R1.6. Enable it as follows:

1. In the Web Admin Interface go to **Configuration > Call Settings** and in the SIP Settings section, set TIP (Telepresence Interoperability Protocol) calls to Enabled.




2. Set both SIP Bandwidth Settings to at least 4000000.




3. Click **Submit**.

## 5.5 IVR Configuration

You can configure an Interactive Voice Response (IVR) to use to manually route to pre-configured calls. Incoming calls can be routed to the IVR where callers are greeted by a prerecorded voice message inviting them to enter the ID number of the call or coSpace that they want to join. Video participants will see a welcome splash screen with the Acano logo. After entering the ID users are routed to the appropriate call or coSpace, or prompted to enter a PIN if the call or coSpace has one. (Callers are disconnected after the third incorrect call ID.)

If you intend to use an IVR follow these instructions:

1. Sign into the Web Admin Interface and go to **Configuration > General**.
2. Configure the following:
   - IVR Numeric ID = numeric call ID that users call to reach the IVR
   - IVR Telephone Number = external phone number that users have to call to reach the IVR
3. Configure the appropriate routing on your SIP Call Control to ensure that calls to the numbers set in the previous step are routed to the Acano server.

Note: In R1.6 there is a new Target IVR settings in the Web Admin Interface **Configuration > Inbound Calls** page.

# 6 Dial Plan Configuration – Integrating Lync

## 6.1 Lync Clients Dialing into a Call on the Acano solution

This section provides the equivalent of the previous section but for Lync endpoints joining a meeting hosted on the Acano solution. It uses the same call number/URI: adapt the example as appropriate.

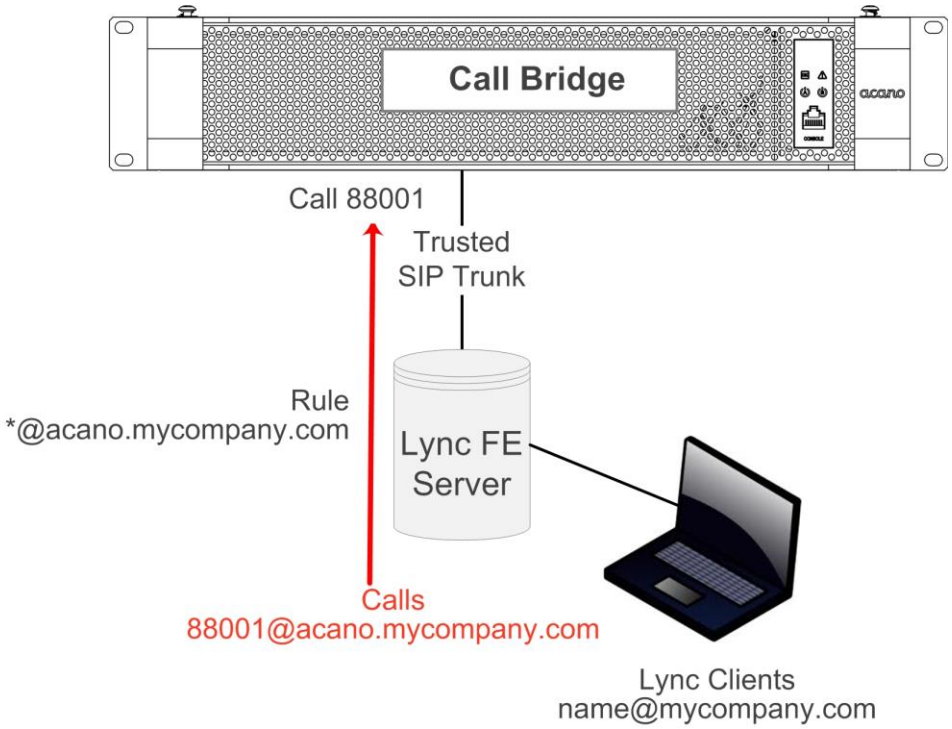



**Figure 8: Example Lync clients calling into Acano server hosted meetings**

### 6.1.1 Lync Front End Server configuration

To route calls originating from Lync clients to the Acano solution:

1. Add a Lync static route pointing to the Acano solution matching domain acano.example.com. See the Appendix with an example for details.

### 6.1.2 Adding a dial plan rule on the Acano solution

1. Sign in to the Web Admin Interface and go to **Configuration > Outbound Calls**.
2. Set up a dial plan rule with:
   - Domain = **mycompany.com**
   - SIP Proxy = the IP address or FQDN of your Lync FE pool or server
   - Local contact domain = **callbridge.acano.mycompany.com**

Note: The local contact domain field should contain the Fully Qualified Domain Name (FQDN) for the Acano server. It should only be set if setting up a trunk to Lync.

- Trunk Type = Lync
- Local From Domain = **acano.mycompany.com**
- Leave SIP Proxy to Use blank

Lync clients can now dial into a call 88001 hosted on the Acano solution by dialing 88001@mycompany.com.

## 6.2 Integrating SIP Endpoints and Lync Clients

To allow both SIP video endpoints and Lync clients to dial into the same meeting, carry out the configuration in both of the previous sections.

Then both SIP video endpoint users and Lync client users can dial <call_id>@acano.example.com to enter the same call.

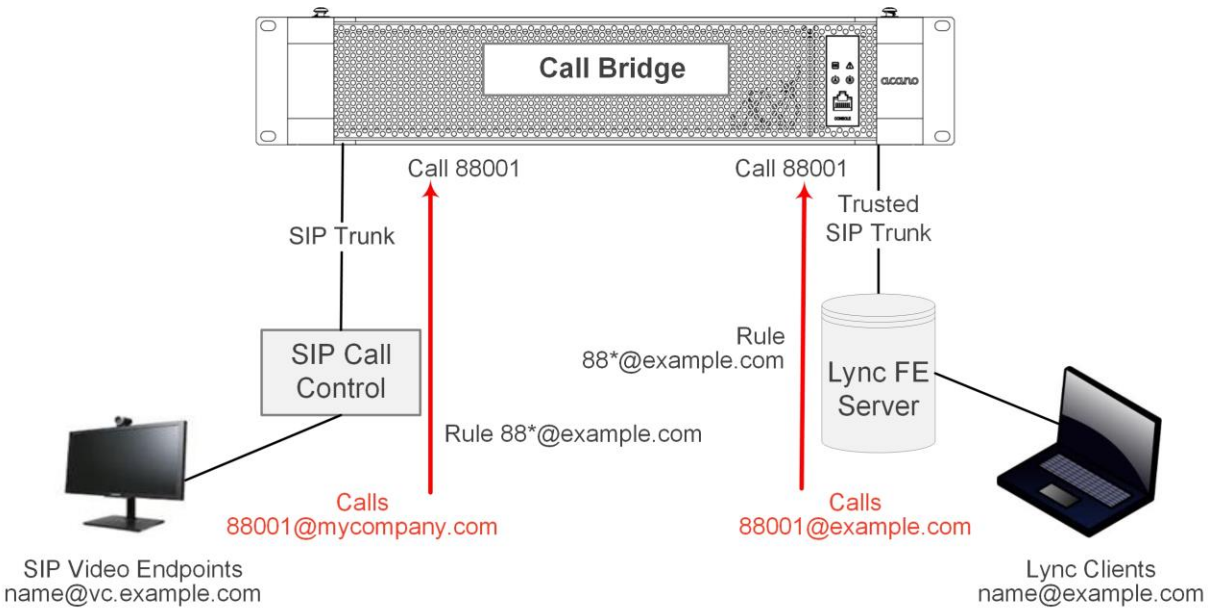



**Figure 9: Example of SIP video endpoints and Lync clients calling into Acano server hosted meetings**

## 6.3 Web Admin Interface Configuration Pages that Handle Calls

Before going on to expand the examples in the previous sections, it is necessary to understand how the Acano solution determines how to handle each call.

Two configuration pages in the Web Admin Interface control how the Acano solution behaves for incoming and outgoing calls: Outbound Calls and Incoming Calls pages. The Outbound Calls page is for outbound calls; the Incoming calls page determines whether incoming calls are rejected. If they are not rejected, but matched and forwarded, then information about how to forward them is required and the Incoming Calls page has two tables – one to configure

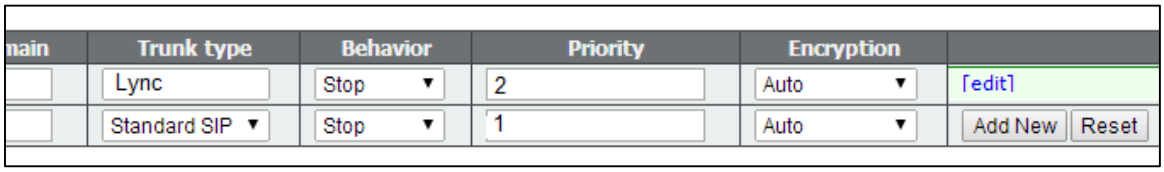
matching/rejection and the other to configure the forwarding behavior. This section provides an overview of these two pages which are then used in the next section to configure the Acano server to act as a gateway between SIP and Lync calls.

### 6.3.1 Outbound Calls page

The Outbound Calls page allows you to configure an appropriate dial plan comprising a number of dial plan rules. The dial plan controls the routing of outbound calls. Each entry/rule in the dial plan matches on the Domain of the outgoing call (see below) and determines which SIP proxy to use (or whether it is a direct call).

The Local Contact Domain is the domain that will be used for the contact URI for calls using this rule. The Local From Domain is the domain the call uses as its originator ID/Caller ID.


**CAUTION**: From R1.2 there has been the ability to configure an explicit contact domain to be used: if you are using Lync, we suggest that you use the Local Contact Domain. If you are not using Lync we recommend that the Local Contact Domain field is left blank to avoid unexpected issues with the SIP call flow.




Usually, you set up rules to route calls out to third party SIP control devices such as Cisco VCS, Avaya Manager or Lync servers. Therefore, there are currently three types of SIP trunks you can configure: Standard SIP, Lync and Avaya.

Note: A common use of the Acano solution is with an Avaya PBX; these calls will be audio-only. However, the Acano solution does not impose this restriction on interoperability with Avaya products (some of which support video also): therefore a call of type of ‘avaya’ does not imply that the call is audio-only.

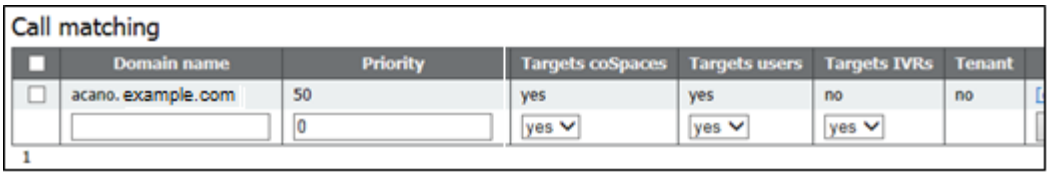
Dial plan rules are tried in the order of the Priority values. In the current Acano solution version only one match is possible for a call and even if there would be other matches in lower priority rules they will not be reached; therefore the Priority is important.

**CAUTION**: The default Encryption behavior mode is Auto. This does not match pre-R1.2 behavior. Previously, all "Lync" outbound dialing rules would automatically use Encrypted mode; therefore you need to ensure that these rules are explicitly set to Encrypted mode to prevent the Call Bridge attempting to use unencrypted TCP for these connections in the event of the TLS connection attempt failing.

### 6.3.2 Incoming Call page: call matching

The top table in the Incoming Call page is the Call Matching table. The rules defined in the Call Matching table govern how the Acano solution handles incoming SIP calls. Any call routed to the Acano server on any domain can be tested for a match for Acano client users or for preconfigured coSpaces on that server.

The example Call matching rule below seeks to match all calls coming in on the **acano.example.com** domain to both Acano users and coSpaces.




For example, if the incoming call was to **name.cospace@acano.example.com** and there was a configured coSpace called **name.coSpace** the call would be routed to the coSpace with that name. If the incoming call was to **firstname.lastname@acano.example.com** the call would be routed to that user with that first and last name.

Alternatively, you can choose not to route calls to users or coSpaces on a per domain basis; that is, you can use one incoming domain for coSpaces and another for users.

After a rule is executed rules further down the list are ignored for the call.

If all Call matching rules fail, the next table, the Call Forwarding table, is used as described in the next section.

Note1: Matching for coSpace and/or users is only done on the part of the URI before the @.

Note2: You cannot configure more than one rule with same destination.

Note3: If the Domain is left blank in a rule, the rule matches any call. If no match is found then the Call Forwarding table is used.

### 6.3.3 Call forwarding

If a call fails to match any of the rules in the Call Matching table in the Incoming Calls page, the call will be handled according to the Call Forwarding table. In this table you can have rules decide whether to reject the call outright or to forward the call in bridge mode. Rules can overlap, and include wildcards. You order rules using the Priority value; higher numbered rules are tried first.

By defining rules, you decide whether to forward the call or not. It might be appropriate to “catch” certain calls and reject them.

For calls that will be forwarded, you can rewrite the Lync destination domain using the Forwarding Domain. A new call is created to the specified domain.

The example Call forwarding rule below forwards calls for the domain **lync.example.com** and the routing is determined by the call routing rules.

Call forwarding

| | Domain matching pattern | Priority | Forward | Caller ID | Rewrite domain | Forwarding domain | |
|---|---|---|---|---|---|---|---|
| | lync. example.com | 50 | forward | pass through | no | | [edit] |
| | | 0 | reject | use dial plan | no | | Add New Reset |

1

If none of the Domain Matching Patterns matches the domain of an incoming call that was not matched in the Call Matching section, the call is terminated.

## 6.4 Adding Calls between Lync Clients and SIP Video Endpoints

This section assumes the configuration described in the two dial plan configuration sections has been completed. It expands the example to allow Lync and SIP video endpoints to dial each other in a call using the Acano server as a gateway to transcode the video and audio (see the figure below).

Note: The Outbound Calls page was used previously to set up a SIP trunk from the Acano server to the Cisco VCS. In order to configure the Acano server to act as a "point-to-point bridge" between Lync and SIP environments, you need to configure call forwarding as described in this section and also set up a SIP trunk from the Acano server to other SIP call control devices you are using such as the Lync FE server (see the appropriate appendix) and CUCM, Avaya CM or Polycom DMA (see the Third Party Deployment Guide).

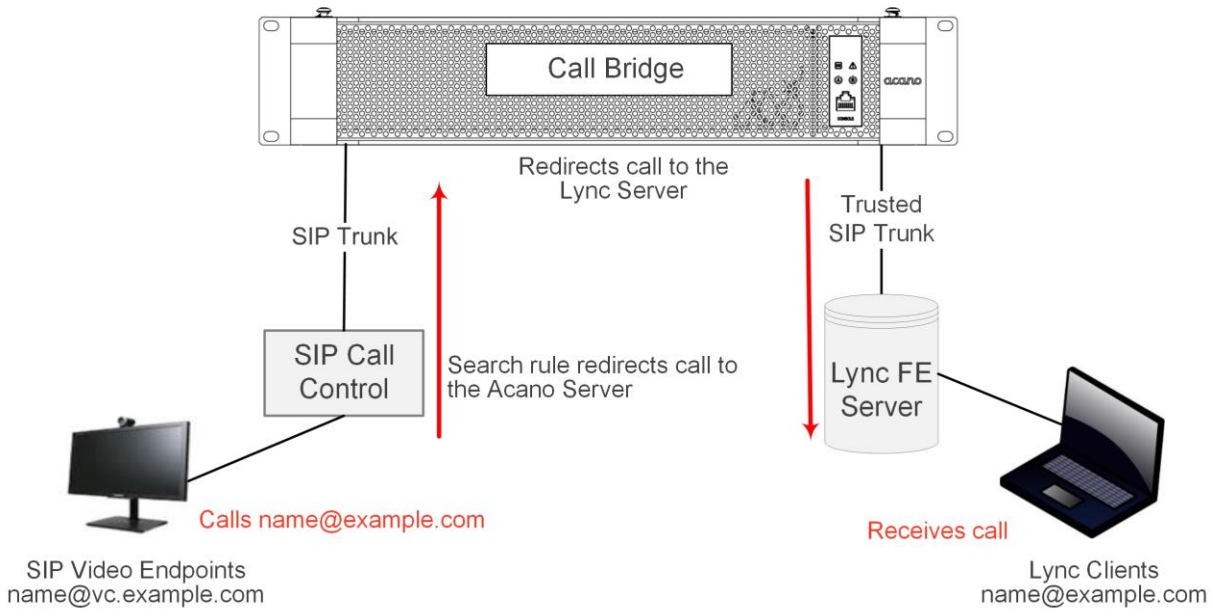



**Figure 10: Example of SIP video endpoints and Lync clients in calls**

In this example:

- A Lync user can dial **<name>@vc.example.com** to set up a call with a SIP video endpoint who is **<name>@vc.example.com**.
- A SIP video endpoint can dial **<name>@example.com** to set up a call with a Lync endpoint who is **<name>@example.com**.

Adapt the example as appropriate.

### 6.4.1 Lync Front End Server configuration

To allow Lync clients to dial SIP video endpoints:

1. Add a Lync static route pointing to the Acano solution for **vc.example.com**.

### 6.4.2 VCS configuration

To route SIP video endpoint calls to Lync clients:

1. Add a search rule on the VCS to route calls with the suffix **@example.com** to the Acano solution.

### 6.4.3 Acano solution configuration

Perform the following steps so that all calls to the Acano solution that are not matched to Acano users or coSpaces are forwarded.

1. Sign in to the Web Admin Interface and go to **Configuration > Incoming Calls**.
2. In the Call Forwarding section, add a new rule as follows:
    - Domain Matching Pattern = *
      Wildcards are permitted in any part of a domain matching pattern.

      (Unmatched calls with a domain that matches this pattern are forwarded using this rule.)
    - Priority: To ensure that this rule is always used, its priority should be the highest of any rules configured (any value, including 0, is acceptable if there are no other forwarding rules configured).

      (Rules are checked in order of priority; highest priority first. If two Domain Matching Patterns would match a destination domain the rule with the higher priority is used.)
    - Forward = forward

      (If you select Reject calls that matched the Domain Matching Pattern are not forwarded but terminate.)
    - Rewrite Doman = no
      The call will be forwarded using the domain that was called.

      (If you select yes here, you must then complete the Forward Domain. The original domain will be replaced with the one you enter in Forward Domain before the call is forwarded.)
3. Click **Add new**.

SIP video endpoints can now call Lync clients by dialing **<name>@example.com**, and Lync clients can call SIP video endpoints by dialing **<endpoint>@vc.example.com**.

## 6.5 Integrating Acano Clients with SIP and Lync Clients

Refer to the LDAP Configuration and Web Admin Interface Settings for XMPP sections for instructions about configuring your Acano solution to use the Acano clients.

If you are using the same LDAP configuration to create both your Lync accounts and Acano clients, problems may occur if a user tries to call a Lync client when using the Acano solution as a gateway because the user may end up calling your Acano XMPP client. The Acano **Configuration > Incoming Calls** page has a table of rules (Call Matching section) to prevent this.

For example, assume you have an account **fred@example.com** on the Acano solution. I also have a **fred@lync.example.com** account on my Lync FE Server. If a call arrives at the Acano solution and no Call Matching rules are configured, the Acano solution will ignore the domain and the call will go to the Acano solution's fred@example.com account. In other words, dialing fred@xxxx will ignore xxxx and see if there is a user "fred" locally.

This is problematic because a user trying to call the Lync address fred@lync.example.com using the Acano solution as a gateway will end up in a call with the Acano XMPP client logged in as fred@example.com. If the same LDAP structure has been used to create both Acano solution's and Lync's user accounts, this will be a common problem.

The solution is to configure the **Incoming Calls** page with the Domain Name field set to something distinct from the domain that the Lync FE server uses. In the example above, a sensible choice for the Domain Name field would be example.com. Then, a call to fred@example.com will reach the Acano client but a call to fred@lync.example.com or fred@xxxx will not. Instead, if the Call Forwarding section is set up, the Acano solution forwards the call on.

## 6.6 Lync Edge Server Integration

### 6.6.1 Lync Edge Call Flow

To establish a call from the Acano server to the Lync Edge server (see the figure below):

1. The Acano Call Bridge makes a "register" SIP call to the Lync FE server.
2. The "register" is acknowledged.
3. The Call Bridge sends a "subscribe" to the Lync FE server.

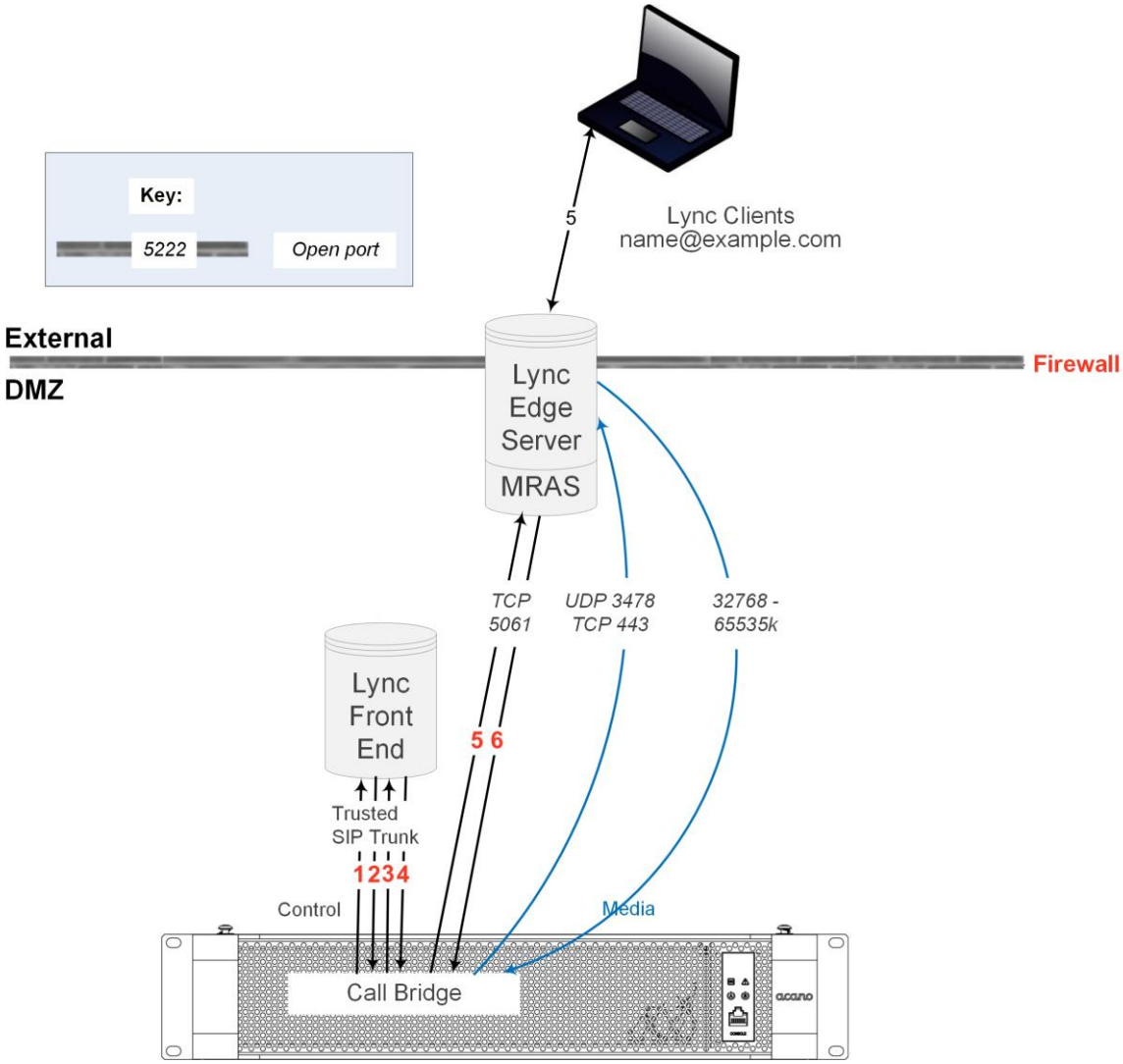



**Figure 11: Call Bridge to Lync Edge Server Call Flow**

4. The Front End server returns the URI of the media relay authentication server (MRAS). (The Lync Edge Server acts as a MRAS.)
5. (and 6) Call Bridge contacts the MRAS over SIP to get the Lync Edge information for the call.

The call media then flows directly between the Call Bridge and TURN server on UDP port 3478 and returns to the Call Bridge on a port in the ephemeral range above.

Therefore the following ports need to be opened in the firewall for the media: UDP 3478 outgoing and 32768-65535 incoming.

### 6.6.2 Configuration for using Lync Edge

To use a Lync Edge server, log in to the Web Admin Interface, go to **Configuration > General** and configure the Lync Edge Settings. (When a Lync Edge server is configured, it takes the TURN / ICE role for Lync calls, and so at some level is an alternative to the TURN Server Settings above.)

You also need to create a Lync user client account to set up the Acano Lync Server Edge configuration.

Follow these steps to set up the Acano solution to use the Lync Edge server:

1. Ensure that you have the appropriate DNS records in place; see the appendix on DNS records for the full requirements.
2. Create a new user in your LDAP directory, just as you would any other user in your directory, i.e. firstname="acano", second name = "edge".
3. Login into the user manager on your Lync Server and create a Lync Client user from the user you created in the previous step. Do thus in the same way as you would any other user to enable them to use Lync. Using the example name above create a Lync client user called **acano.edge@lync.example.com**
4. Sign in to the Web Admin Interface, and go to **Configuration > General.** Configure the Lync Edge Settings by entering the Lync FE Server Address (or a host name that resolves to this). For Username enter the Lync client user name created in the previous step.
5. Complete the Number of Registrations field, if necessary.

   This field overcomes a feature of the Lync Edge server that limits the number of simultaneous calls that it will run for one registered device. By entering a number greater than 1, the Call Bridge will make that number of registrations, thereby increasing the number of simultaneous calls that the Acano solution can make out through the Lync Edge Server.

   Entering a number greater than 1 adds a number to the end of your Lync Edge username and registers with the resulting username. For example, if you configured Username as edgeuser@example.com and set Number of Registrations to 3, you will need to create the following users in your Lync environment so that they can be used with the Edge server;

   `edgeuser1@example.com`

   `edgeuser2@example.com`

   `edgeuser3@example.com`

   We recognize that this requires some administrative overhead; however it is due to a limitation of the Lync Edge server as explained above.

   Leave the Number of Registrations blank to only make a single registration as `edgeuser@example.com`.

---

Note: The Acano solution supports Lync content (presentations contributed over RDP) from external Lync clients whose media arrives via the Lync Edge server. In addition, coSpace (URIs) now report back as busy or available based on how many participants are currently in the coSpace so that Lync clients that have Acano coSpaces in their favorites can see the coSpace status.

Note: Acano clients continue to use the Acano TURN Server even if a Lync Edge server is configured.

Note: If you have a Lync Edge server configured, all Lync calls will use that server for ICE candidate gathering and external media connectivity. If you do not have a Lync Edge server configured, Lync calls handled by the Acano solution will use any configured TURN server.

---

## 6.7 Lync Federation

Acano solution R1.6 adds support for federation with Microsoft Lync. This allows calls to be made from the Acano server to any Lync domain and vice versa.

To allow inbound calls you must:

1. create the DNS SRV record _sipfederationtls._tcp.domain.com that points to the FQDN of the Acano server. This step is required as Call Bridge will need to have a public IP, and NAT is not supported in this scenario.
2. add a DNS A record that resolves the FQDN of the Acano server to a public IP address.
3. upload a certificate and certificate bundle to the Acano server that complies with the following:
   a. the certificate must have the FQDN as the CN, or if using a certificate with a SAN list then ensure that the FQDN is also in the SAN list. Note: if the certificate contains a SAN list, then Lync will ignore the CN field and only use the SAN list.
   b. the certificate must be signed by a real CA.
   c. the certificate bundle must contain the Root CA's certificate and all intermediate certificates in the chain in sequence, so that a chain of trust can be established.

   Note: for more information on certificates refer to the Introduction in the Acano Certificate Guidelines.

4. Open the appropriate Firewall ports as stated in the Acano Deployment Guide for example: TCP 5061, UDP 3478, UDP 32768-65535, TCP 32768-65535

For outbound calls from Acano:

5. create an outbound dial rule, leave the Domain and SIP proxy fields blank, and set Trunk type as Lync. Also set the appropriate Local contact domain and the Local from domain fields.

# 7 Web Admin Interface Settings for XMPP

This section explains how to configure the settings through which the Call Bridge communicates with XMPP server.

Note: If you are not using the Acano clients including the WebRTC Client, skip this section.

## 7.1 Network Topology

The following diagram shows a possible network topology and is used for the examples in this section.

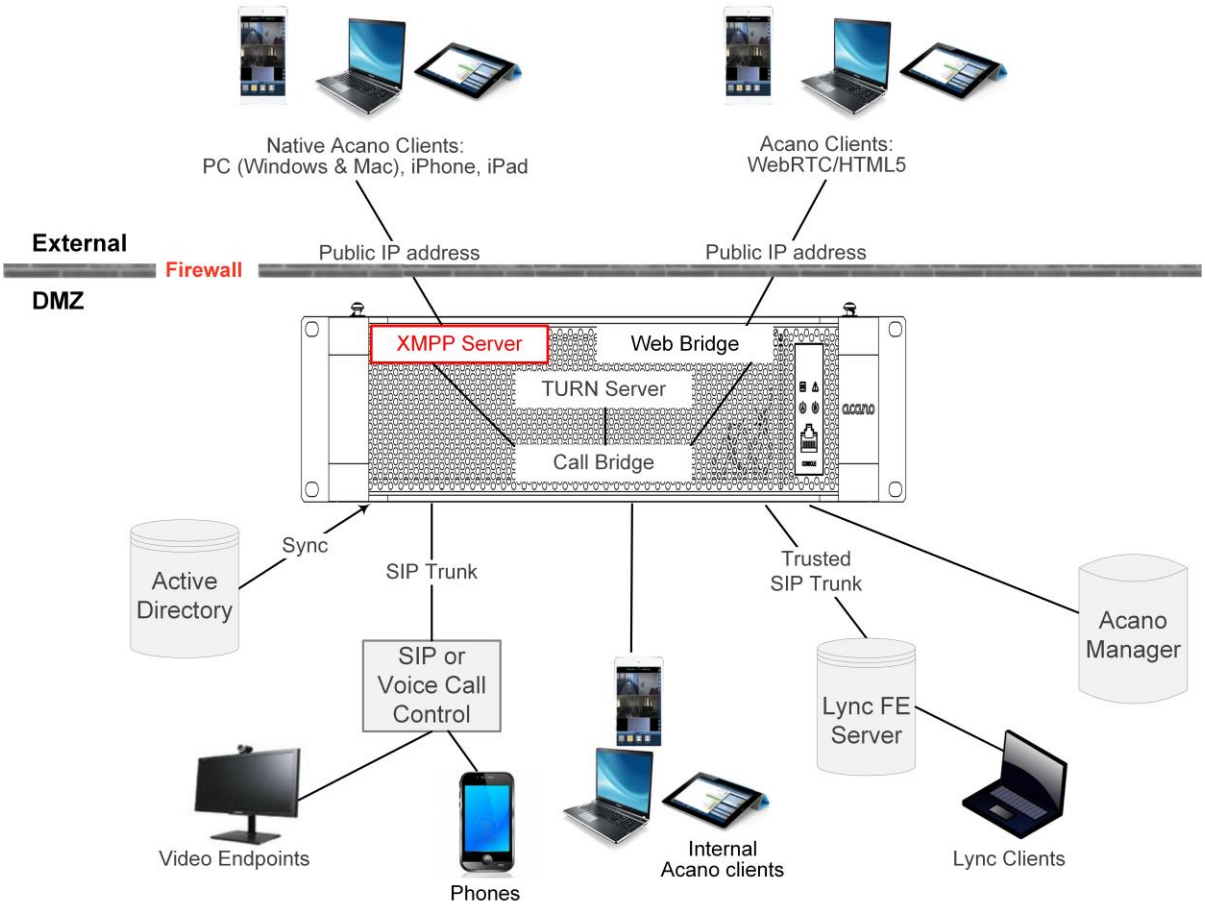
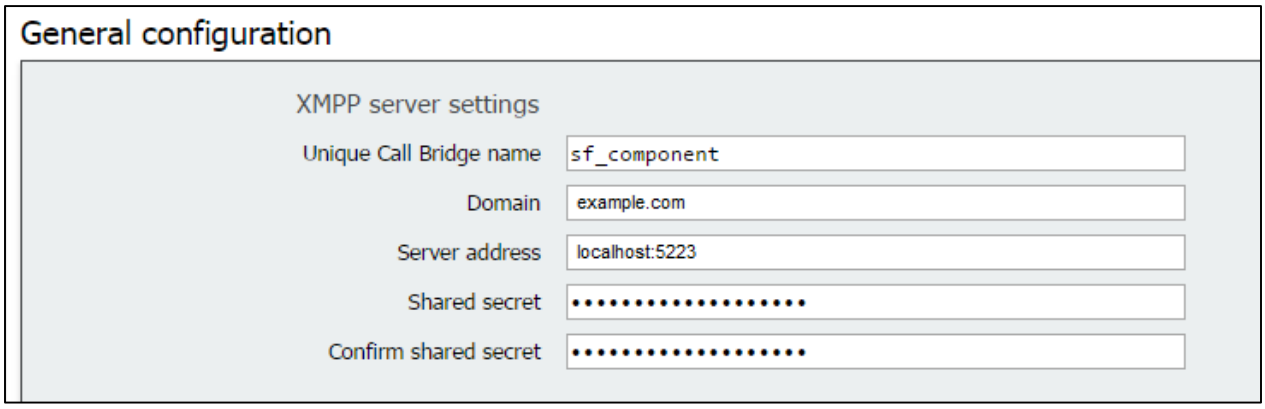



**Figure 12: Example network topology showing XMPP server**

## 7.2 XMPP Settings

1. Ensure that you have installed a security certificate for the XMPP server.
2. Ensure that you have configured the XMPP server.
3. If you are using a virtual host, ensure that you have uploaded the license key file.

4. Log in to the Web Admin Interface and configure the XMPP server settings as follows:
   a. Go to **Configuration > General**

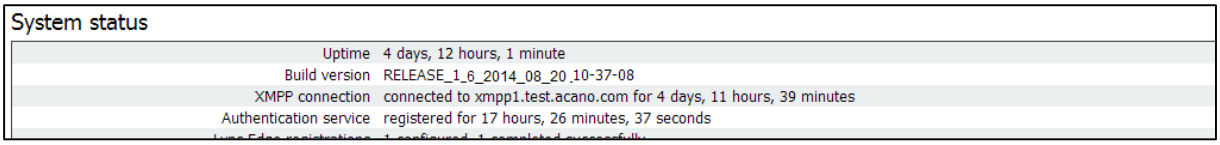



   b. Configure the XMPP Server Settings section using the domain, component and secret set up earlier. The Unique Call Bridge name is the component name set up previously (without a domain suffix). The Server Address is the IP address or hostname of the XMPP server, with an optional :<port> (default is 5223).

Note: Authentication Proxy component and Authentication suffix which were used in release 1.2 and earlier, are no longer required.

   c. Select **Submit** at the bottom of this page.

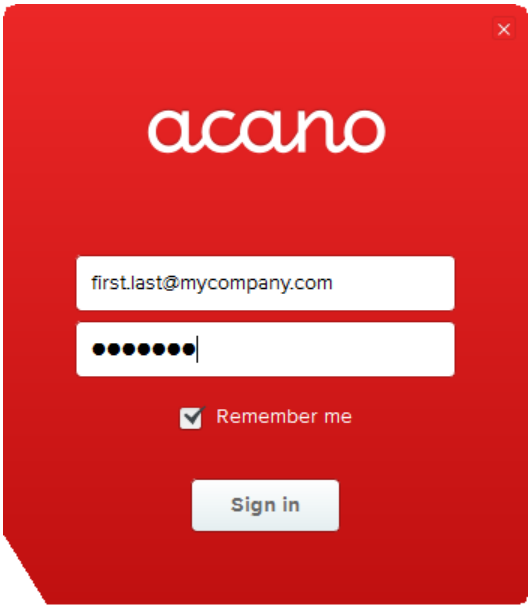
5. Go to **Status > General** and verify the server connection.
   You should see details similar to the following in the XMPP Connection field:




6. On a PC, install the Acano PC Client from:

   https://clientupgrade.acano.com/download/oBklj0sd28dl2mz/AcanoClient.application

   Log in to the Acano PC Client using one of the newly created user accounts. Then check that you can make calls as expected.




## 7.3 Client-based coSpace Creation and Editing

PC Client users can create coSpaces. These coSpaces have URIs and IDs by default, allowing them to be easily dialed by SIP endpoints. The SIP dial-in URI is automatically created; however, you can enter a preferred SIP URI and the Acano solution will automatically ensure that it is a unique URI for the domain assuming this is a single server deployment. This means users can now create coSpaces and email the SIP URI so that others can join. This makes it straightforward to bring SIP endpoints into your coSpace.

PC Client users can click the “i” button for a coSpace; this displays the Call ID number. Emailing this Call ID to guest users allows them to join the coSpace using the web link you have configured (see the next section). Alternatively, PC Client users can copy the full web link in the coSpace information by right-clicking and email it to guests. This link bypasses the guest “call ID” page above, going directly to the guest identification page.

Note: coSpaces can also be created from the Acano solution API (see the API Reference) and in the Web Admin Interface **Configuration > coSpaces** page.

# 8 Web Admin Interface Settings for the Web Bridge

This section explains how to configure the settings through which the Call Bridge communicates with the Web Bridge server. This allows you to use WebRTC video calls and meetings.

If you are testing the WebRTC client, follow the instructions below in the order provided at any time after the initial Acano solution configuration has been completed. If you are not using this Acano client, skip this section.

## 8.1 Network Topology

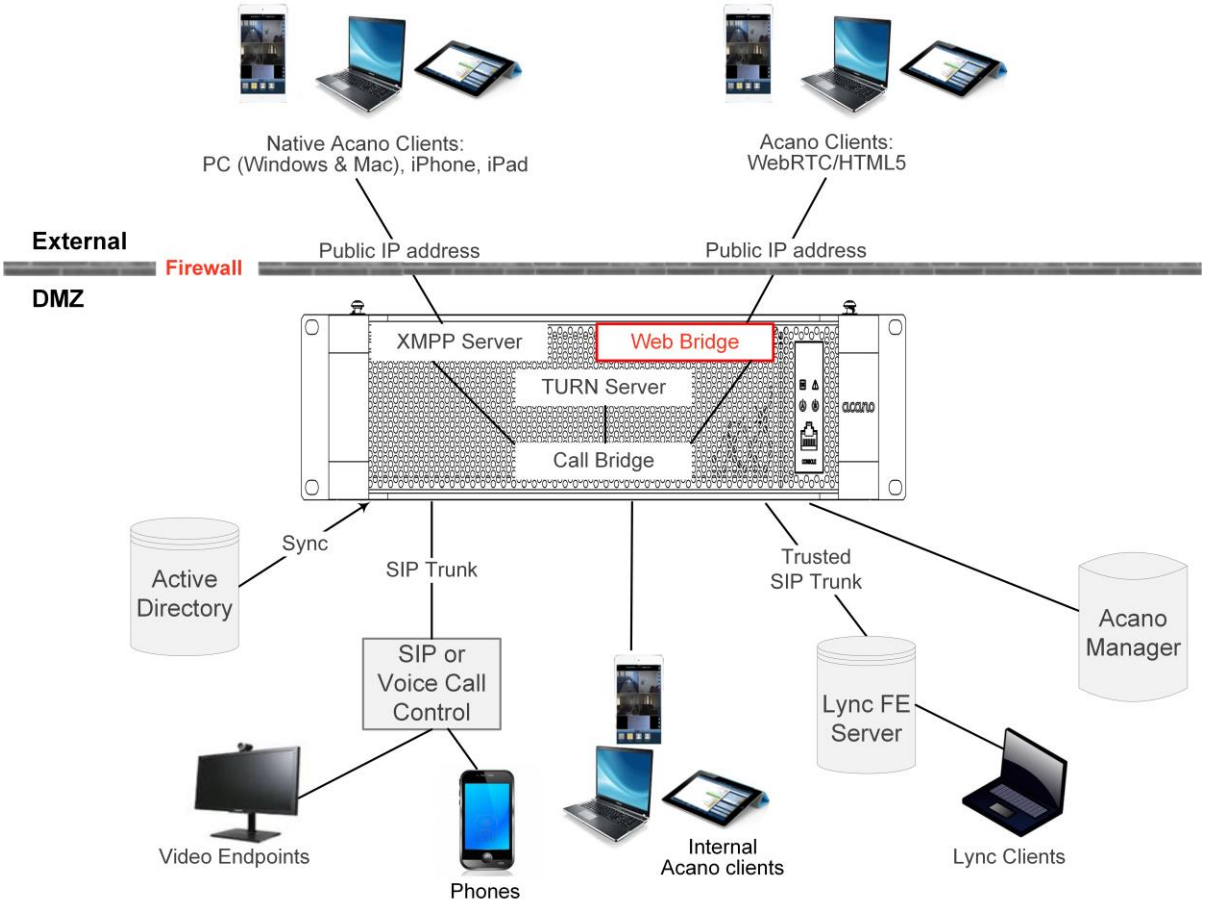



**Figure 13: Example network topology showing Web Bridge**

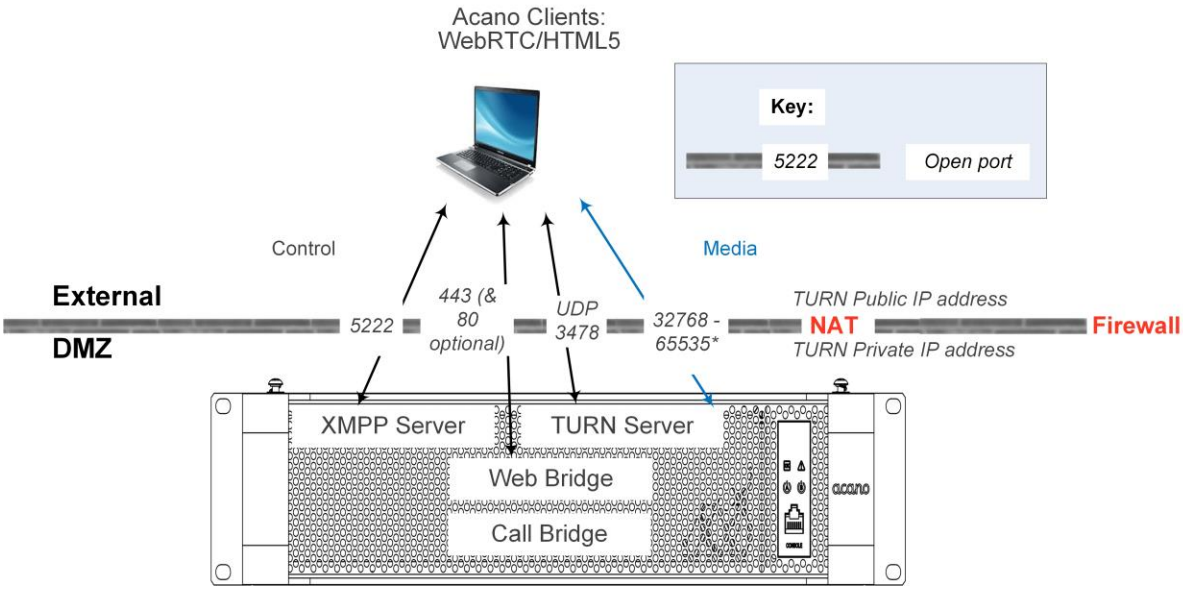



**Figure 14: WebRTC Client port usage**

Note: * Although the port range between the TURN server and the External clients is shown as 32768-65535, currently only 50000-51000 is used. The required range is likely to be larger in future releases.

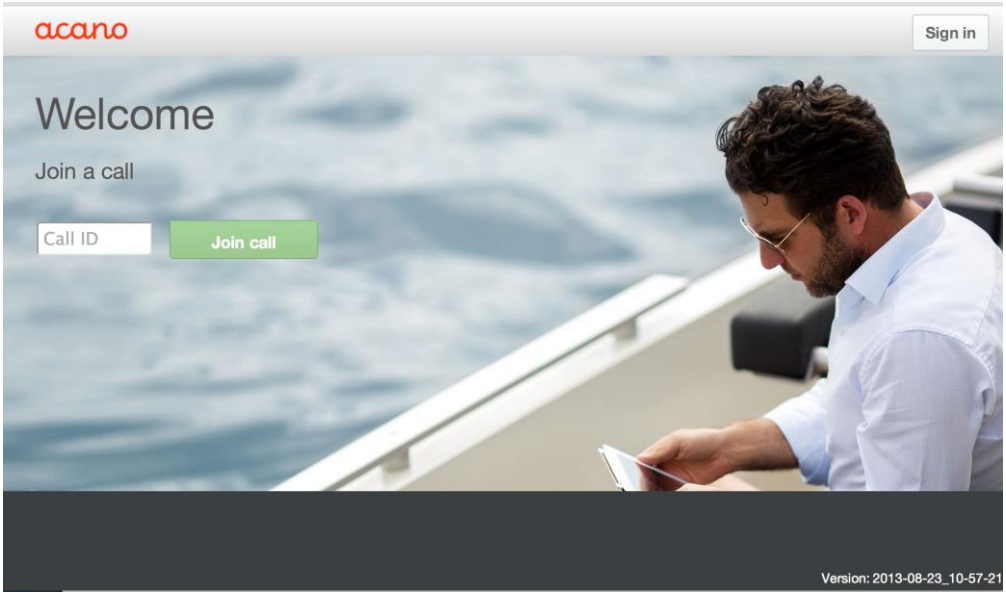
## 8.2 Web Bridge Settings

Follow the steps in order.

1. Ensure that you have installed the Web Bridge certificate and license.
2. Ensure that you have configured the Web Bridge.
3. Sign in to the Web Admin Interface and configure the Acano solution as follows:
   - Go to **Configuration > General**.
   - Set the following where:
     - Guest Account Client URI = The URI including https:// to reach the guest account; for example, https://join.example.com
     - Guest Account JID Domain = guest account JID, e.g. example.com


4. Open a web browser and go to https://join.example.com to test the configuration.

Guest users selecting the general configured web link will see a landing page in which they can enter the Call ID to join a call.




In addition, Acano users who do not have access to a native Acano client but have an account can select the login link in the top right hand corner of the screen to sign in as they would on a native client. After signing in they see their coSpaces, and can invite participants and participate in meetings - all from the WebRTC Client.

Note: Acano clients can be downloaded at: [www.acano.com/help](www.acano.com/help)

- PC Client ClickOnce
- Mac Client DMG download
- iOS Client download

# 9 Web Admin Interface Settings for the TURN Server

This section explains how to configure the settings through which the Call Bridge communicates with the TURN server. The TURN server allows you to use the built-in firewall traversal technology when traversing a firewall or NAT.

Follow the instructions below in the order provided at any time after the initial Acano solution configuration has been completed.

## 9.1 Network Topology

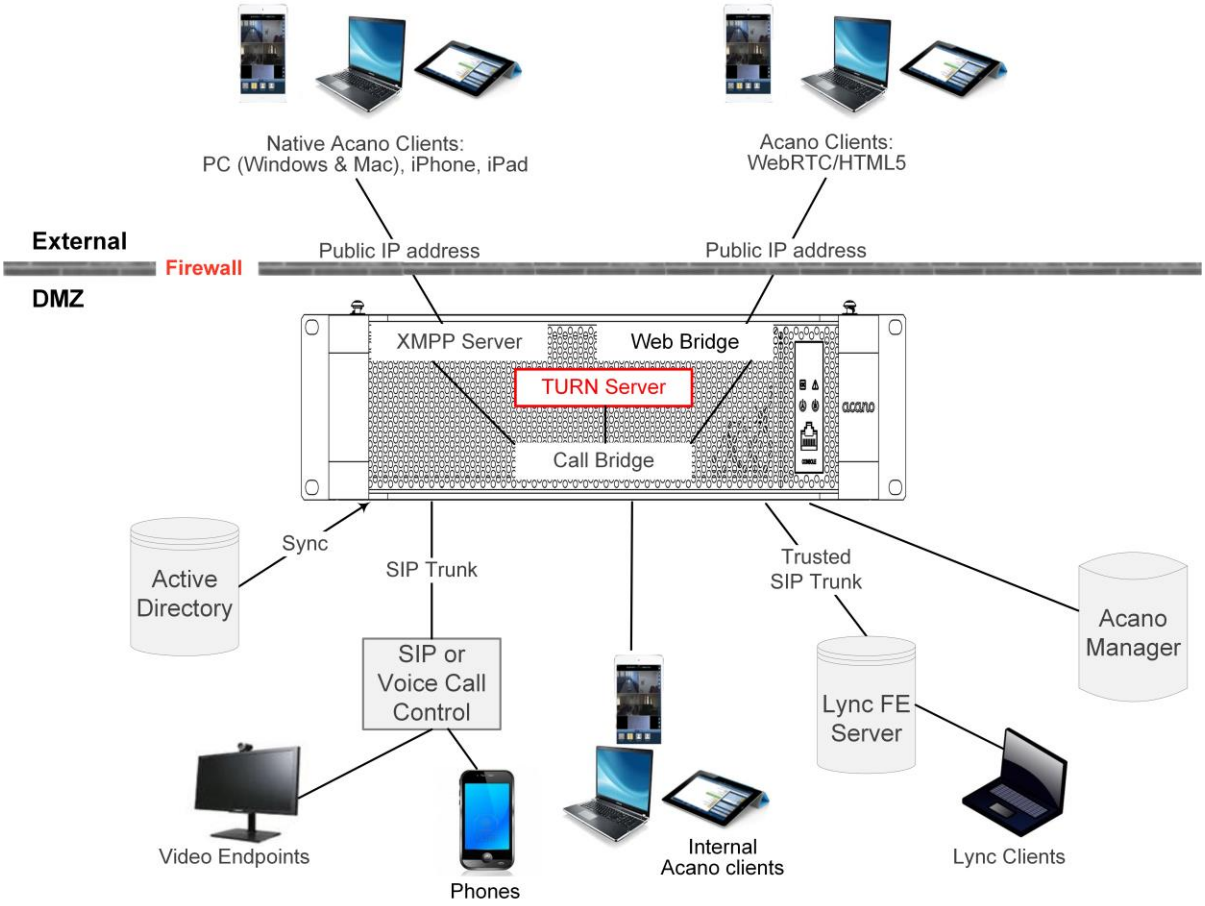



**Figure 15: Example network topology showing TURN Server**

## 9.2 TURN Server Settings

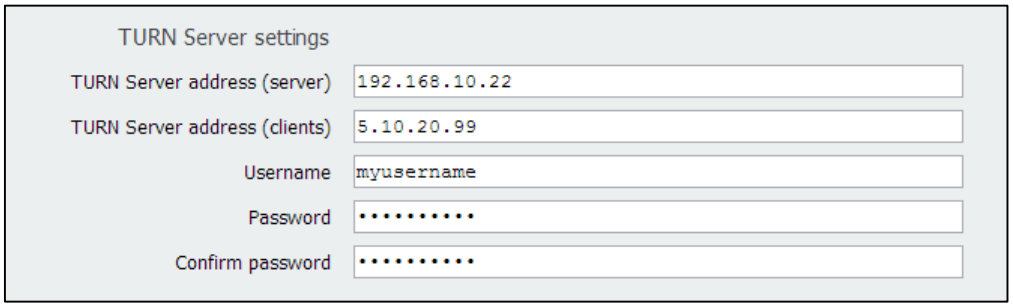
Follow the steps in order.

1. Ensure that you have [configured the TURN server.]
2. Log in to the Web Admin Interface and configure the Acano solution as follows:

- Go to **Configuration > General**.
- Set the following:
  - TURN Server Address (Server) = internal server IP address that the Call Bridge will use to access the TURN server to avoid firewall traversal for internal call control
  - TURN Server Address (Clients) = public IP address assigned to the TURN server that external clients will use to access the TURN server. This will be the IP address entered in earlier when you configured the TURN server.

    Notes:

    - For example if the interface of the TURN Server is on IP address XX.XX.XX.XX and NAT'ed to an external IP address YY.YY.YY.YY then enter XX.XX.XX.XX as the TURN Server Address (Server) and YY.YY.YY.YY as TURN Server Address (Client). If the interface is on the external IP then no need to enter a client address
    - You can enter a DNS name instead of an IP address in both fields, if the DNS name resolves to the appropriate IP address
    - If you are using a public IP address, leave TURN Server Address (Clients) address blank and set TURN Server Address (Server) to the public IP address or DNS name used
  - Username and Password = your information



# 10 Additional Security Considerations & QoS

A number of security issues have already been discussed (e.g. certificates) but the Acano solution 1.6 offers a number of additional functions for securing your deployment, as described in this section.

## 10.1 Common Access Card (CAC) integration

The Common Access Card (CAC) is used as an authentication token to access computer facilities. The CAC contains a private key which cannot be extracted but can be used by on-card cryptographic hardware to prove the identity of the cardholder. The Acano solution 1.6 supports administrative logins to the SSH and Web Admin Interface using CAC.

The MMP commands available are (also see the MMP Command Reference):

- `cac enable|disable [strict]`: enables/disables CAC mode with optional strict mode removing all password-based logins
- `cac issuer <ca cert-bundle>`: identifies trusted certificate bundle to verify CAC certificates
- `cac ocsp certs <key-file> <crt-file>`: identifies certificate and private key for TLS communications with OCSP server, if used
- `cac ocsp responder <URL>`: identifies URL of OCSP server
- `cac ocsp enable|disable`: enables/disables CAC OCSP verification

## 10.2 Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is a mechanism for checking the validity and revocation status of certificates. The MMP can use OCSP to work out whether the CAC used for a login is valid and, in particular, has not been revoked.

## 10.3 FIPS

You can enable a FIPS 140-2 level 1 certified software cryptographic module, then cryptographic operations are performed using this module and are restricted to the FIPS-approved cryptographic algorithms.

The MMP commands are (also see the MMP Command Reference):

- `fips enable|disable`: enables/disables the FIPS-140-2 mode cryptography for all cryptographic operations for network traffic. After enabling or disabling FIPS mode, a reboot is required
- `fips`: displays whether FIPS mode is enabled
- `fips test`: runs the built-in FIPS test

## 10.4 TLS Certificate Verification

You can enable Mutual Authentication for SIP and LDAP in order to validate that the remote certificate is trusted. When enabled, the Call Bridge always asks for the remote certificate (irrespective of which side initiated the connection) and compares the presented certificate to a trust store that has been uploaded and defined on the Acano server.

The MMP commands available are (also see the MMP Command Reference):

- `tls <sip|ldap> trust <crt bundle>`: defines Certificate Authorities to be trusted
- `tls <sip|ldap> verify enable|disable|ocsp`: enables/disables certificate verification or whether OCSP is to be used for verification
- `tls <sip|ldap>`: displays current configuration

## 10.5 User Controls

MMP admin users can:

- Reset another admin user's password
- Set the maximum number of characters that can be repeated in a user's password – and there are a number of other user password rule additions
- Limit MMP access by IP address
- Disable MMP accounts after configurable idle period

## 10.6 Firewall Rules

In release 1.6 the MMP supports the creation of simple firewall rules for both the media and admin interfaces. Note that this is not intended to be a substitute for a full standalone firewall solution and therefore is not detailed here. Firewall rules must be specified separately for each interface. See the MMP Command Reference for full details and examples.

**CAUTION**: We recommend using the serial Console port to configure the firewall, because using SSH means that an error in the rules would make the SSH port inaccessible. If you must use SSH, then ensure that an `allow ssh` rule is created for the ADMIN interface before enabling the firewall.

## 10.7 DSCP

You can enable DSCP tagging for the traffic types on the Acano server (see the MMP Command Reference).

1. Sign in to the MMP and set the DSCP values as required.
2. Go to **Configuration > Call Settings** and set the DSCP Mode as follows:
   - In a non-AS SIP environment, select Use Normal Values
   - In an AS SIP environment, select Use Assured Values

Note: DSCP tagging is for all packets being sent from the Acano solution only. For PC Client DSCP tagging, Group Policy must be used to define desired DSCP values because Windows controls this, and normal user accounts have no permissions to set DSCP.

# Appendix A DNS Records Needed for the Acano Solution

Note: You can configure the DNS resolver(s) to return values which are not configured in external DNS servers or which need to be overridden; custom Resource Records (RRs) can be configured which will be returned instead of querying external DNS servers. (The RR is not available to clients.) See the MMP Command Reference for details.

Note: Verify that no DNS A or SRV records already exist for your Acano servers before defining the records below.

| Type | Example | Resolves to | Description |
|---|---|---|---|
| SRV(*) | _xmpp-client._tcp.example.com | The A record xmpp.example.com below. Usually this is port 5222 | Used by clients to login. The SRV record must correspond to the domain used in your XMPP usernames |
| SRV(*) | _xmpp-server._tcp.example.com | The A record xmpp.example.com below. Usually this is port 5269 | Used to federate between XMPP servers. The SRV record must correspond to the domain used in your XMPP usernames |
| A | xmpp.example.com | IP address of the XMPP server | Used by clients to login. |
| A / AAAA | join.example.com | IP address of the Web Bridge | This record is not used by the Acano solution directly; however, it is common practice to provide an end user with an FQDN to type into the browser which resolves to the Web Bridge. There is no restriction or requirement on the format of this record. |
| A / AAAA | uk.example.com | IP address of the Call Bridge | Used by the Lync FE server to contact the Call Bridge |
| A / AAAA | ukadmin.example.com | IP address of the Web Admin Interface | This record is used purely for admin purposes; when system administrators prefer a FQDN to remember for each MMP interface |

(*) SRV records do not resolve directly to IP addresses. You need to create associated A or AAAA name records in order to satisfy the SRV requirements

# Appendix B Ports Required

The following diagram labels the links on which ports need to be open and shows which firewall is concerned in a single combined server deployment.

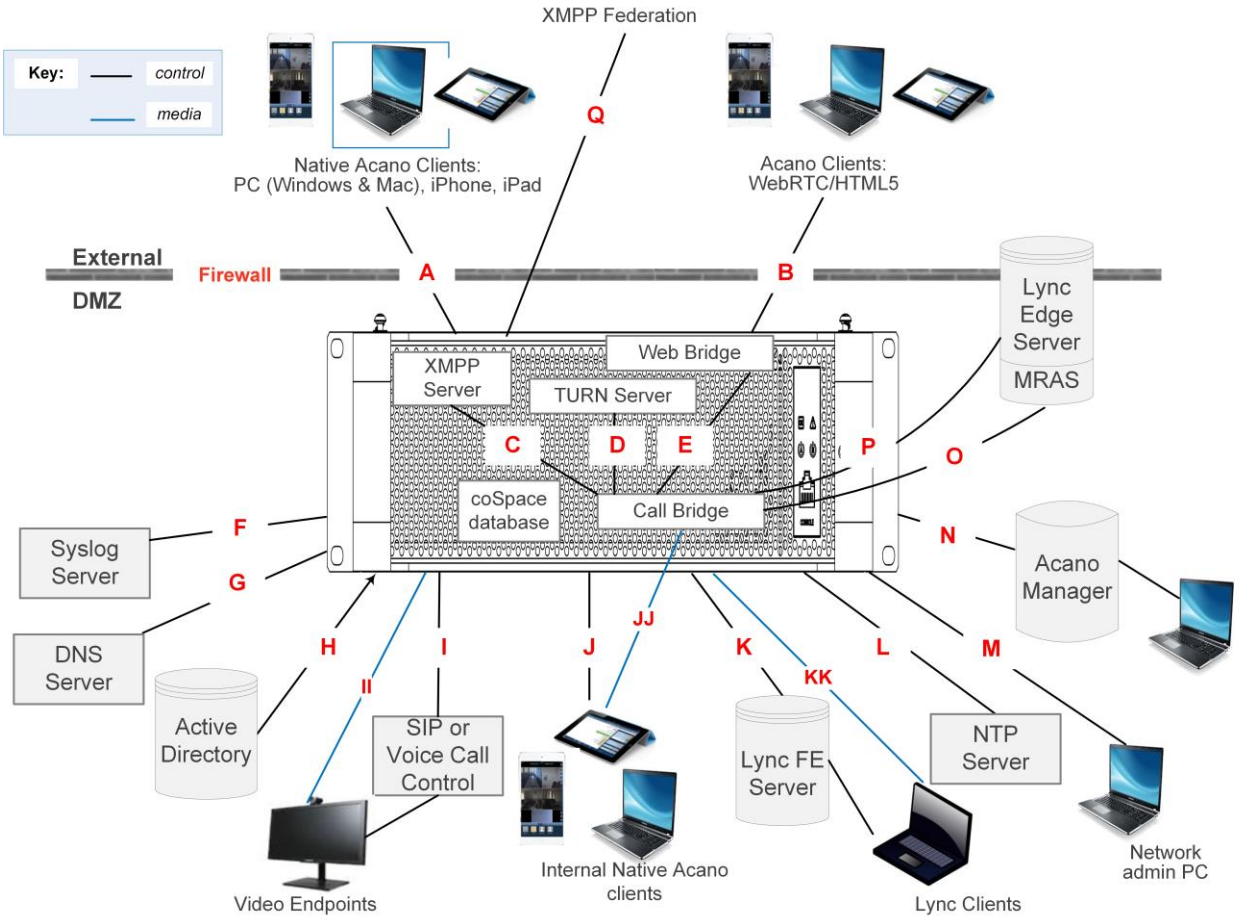



**Figure 16: Ports that must be open in an Acano solution deployment**

The following ports are required by the Call Bridge.

| Function | Destination Port | Type | Direction | Used on Link(s) | Configurable ? |
|---|---|---|---|---|---|
| HTTP | 80 | TCP | Incoming | M | MMP |
| HTTPS | 443 | TCP | Incoming | M, N | MMP (for M) |
| HTTPS | 443 | TCP | Outgoing | N | |
| SIP UDP | 5060 | UDP | Both | I, JJ | |
| SIP TCP | 5060 | TCP | Both | I, JJ | |

| | | | | | |
|---|---|---|---|---|---|
| SIP TLS | 5061 | TCP | Both | I, JJ, K, O | |
| SIP BFCP | 32768-65535 | UDP | Incoming | I, JJ | |
| SIP BFCP | 1024-65535# | UDP | Outgoing | I, JJ | |
| API HTTPS | 443 | TCP | Incoming | M | |
| TURN | 3478 | UDP | Outgoing | P | |
| TURN | 443 | TCP | Outgoing | P | |
| STUN/RTP | 32768-65535 | UDP | Incoming | I, JJ, K | |
| STUN/RTP | 32768-65535 | UDP | Incoming | P | |
| STUN/RTP | 1024-65535 # | UDP | Outgoing | I, JJ, K | |
| RDP | 32768-65535 | TCP | Incoming | K | |
| RDP | 1024-65535 ++ | TCP | Outgoing | K | |
| LDAP/LDAPS + | 636/389 | TCP | Outgoing | H | Web Admin Interface |
| DNS | 53 | UDP | Outgoing | G | |
| CDR | Set in Web Admin Interface | TCP | Outgoing | N | Web Admin Interface |

*+ Ports 389 and 636 (secure) are commonly used for this function but the port is configurable. (The same applies to 3268 and 3269 (non-secure and secure) global catalog LDAP requests.)*

*++ Exact range depends on configuration on Lync server*

*# Exact range depends on far end*

The following ports are used by MMP.

| Function | Destination Port | Type | Direction | Used in Link(s) | Configurable ? |
|---|---|---|---|---|---|
| SSH | 22 | TCP | Incoming | M | |
| Syslog | 514 | TCP | Outgoing | F | MMP |
| NTP | 123 | UDP | Outgoing | L | |
| SNMP | 161 | UDP | Incoming | | |
| SNMP | 162 | UDP | Outgoing | | |

The following ports are used by the Web Bridge

| Function | Destination Port | Type | Direction | Used in Link(s) | Configurable ? |
|---|---|---|---|---|---|
| HTTP | 80 | TCP | Incoming | B | MMP |
| HTTPS | 443 | TCP | Incoming | B | MMP |

The following ports are used by the XMPP Server

| Function | Destination Port | Type | Direction | Used in Link(s) | Configurable ? |
|---|---|---|---|---|---|
| XMPP Client | 5222 | TCP | Incoming | A, J | |

The following ports are used by the TURN Server

| Function | Destination Port | Type | Direction | Used in Link(s) | Configurable ? |
|---|---|---|---|---|---|
| STUN | 3478 | UDP | Incoming | A, B | |
| STUN RTP | 32768-65535* | UDP | Incoming | A, B | |

Note: * Although the range between the TURN server and the external Acano clients is shown as 32768-65535, currently only 50000-51000 is used. A wider range is likely to be required in future releases.

# Appendix C Example of Configuring a Static Route from a Lync Front End Server

**Important Note**: This appendix provides an example to be used as a guideline and is not meant to be an explicit set of instructions for you to follow. Acano strongly advises you to seek the advice of your local Lync server administrator on the best way to implement the equivalent on your server's configuration.

1. Ensure that you have installed certificates on the Acano solution to trust the Lync server – as described earlier in this document.

## Lync Configuration Changes

2. Optionally, enable HD720p on Lync as follows (if you want HD calls from Lync because the default is VGA):
   a. Open the Lync Server Management Shell,
   b. Enable support for HD720P Lync calls with:
   ```
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
   ```
3. Add the trusted application and static routes to the Acano solution with the following five commands:
   ```
   New-CsTrustedApplicationPool -Identity acano-trust -ComputerFqdn
   fqdn.acanoserver.com -Registrar fqdn.lyncserver.com -site 1 -
   RequiresReplication $false -ThrottleAsServer $true -
   TreatAsAuthenticated $true
   ```
   Replacing
   - acano-trust with a name of your choice
   - fqdn.acanoserver.com with the FQDN of the Acano solution
   - fqdn.lyncserver.com with your Lync FE Server or Pool FQDN

   ```
   New-CsTrustedApplication -ApplicationId acano-application -
   TrustedApplicationPoolFqdn acano-trust -Port 5061
   ```
   Replacing
   - acano-application with name of your choice
   - acano-trust with name used above

   ```
   $x=New-CsStaticRoute -TLSRoute -Destination "fqdn.acanoserver.com" -
   MatchUri "something.com" -Port 5061 -UseDefaultCertificate $true
   ```
   Replacing
   - fqdn.acanoserver.com with your FQDN of the Acano solution

- something.com with the URI match of your choosing, possibly acano.yourcomany.com if that is the domain used for all Acano calls

```
Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x}
Enable-CsTopology
```

This command enables the new topology. Users may have to logout and login again to update to the new HD720p setting, all other settings are automatic and should work within a few minutes.

## Acano Solution Configuration

1. In the Web Admin Interface go to **Configuration > Outbound Calls**
2. In the blank row, for Domain, enter the Lync domain that will be matched for calls that need to be sent to Lync
3. For SIP Proxy to Use, do one of the following:
   - Leave this field blank and the server will perform a DNS SRV lookup for the called domain using _sipinternaltls._tcp.<yourlyncdomain>.com
   - Enter the Front End Pool (or Lync sip domain) and the server will first perform a DNS SRV lookup for that defined domain using _sipinternaltls._tcp.<yourlyncdomain>.com and then perform a DNS A record lookup for the Host entered if the SRV lookup fails to resolve
   - Enter the IP address of your Lync Front End server
4. For Local Contact Domain, enter the FQDN of your Acano solution. (The only case in which this field should be set is when setting up a trunk to Lync; otherwise it should be left blank.)
5. For Local From Domain, enter the domain that you want the call to be seen as coming from (the Caller ID) e.g. **acano.yourcompany.com**

   Note: If you leave Local From Domain blank, the domain used for the Caller ID defaults to that entered as the Local Contact Domain.

6. For Trunk Type, select Lync.
7. Select **Add New**.

After completion you should be able to call from the Lync environment to the Acano solution and from the Acano solution to Lync.

# Appendix D More information on LDAP field mappings

This section provides additional information for LDAP field mappings that you set up for the Acano solution.

Parts of an LDAP field value can be substituted by means of a sed-like construction, as follows:

`$<LDAP field name>|'/<regex>/<replacement format>/<option>'$`

- `<option>` can be g, to replace every match of `<regex>` with `<replacement format>`, or blank to match only the first
- parts of `<regex>` can be tagged for use in `<replacement format>` by enclosing them in round brackets
- tagged matches can be referenced in `<replacement format>` as \x where x is a digit from 0 to 9. Match 0 corresponds to the entire match, and matches 1-9 the 1st to 9th tagged sub-expressions
- single quotes inside the substitution expression must be escaped with a backslash, as must backslash characters themselves
- any character other than a single quote, a backslash, or the digits 0-9 can be used in place of the forward slash that separates the components of the substitution expression
- if the separating character is to be used as a literal within the expression, it must be escaped with a backslash

As an example, the following would convert

**`firstname.lastname@test.example.com`**

addresses into

**firstname.lastname@xmpp.example.com JIDs**

**`$mail|'/@test/@xmpp/'$`**

and the following would remove every lower case 'a' from the user's full name

**`$cn|'/a//g'$`**

A sensible set of expressions for use might be:

| | |
|---|---|
| **Full name:** | **`$cn$`** |
| **JID:** | **`$mail|'/@test/@xmpp/'$`** |
| **CoSpace URI:** | **`$mail|'/@.*//'$.cospace`** |
| **CoSpace dial-in number:** | **`$ipPhone$`** |

# Appendix E Using a Standby Acano Server

The instructions in this appendix apply to both Acano X series and virtualized deployments.

## Backing Up the Currently Used Configuration

1. Establish an SSH connection to the currently used Acano server using an SSH utility such as OpenSSH or PuTTY.
2. Issue the command

   ```
   backup snapshot <name>
   ```

   This backup includes IP addresses, passwords and certificates into a file called name.bak. We recommend using a name in the format servername_date (for example, example_server_2014_09_04)

   A successful backup creation returns:

   ```
   acano> backup snapshot      _server_2014_09_04
   _server_2014_09_04.bak ready for download
   ```
3. Download the backup file using an SFTP client (e.g. WinSCP).

Note: We recommend backing up your Acano solution servers regularly, e.g. once a day and that you store copies of the backup externally to the Acano solution and the standby server.

## Transferring a Backup to the Standby Server

We recommend that you keep the standby sever running at all times.

1. Copy all the certificates and the license.dat file from the standby server in case they differ from the original server that the backup was created on. Store them somewhere safe.
2. Establish an SFTP connection with the standby server.
3. Upload the previously saved backup file on to the standby server.
4. Issue the MMP `backup list` command to confirm that the backup file was successfully uploaded. This should return something similar to:

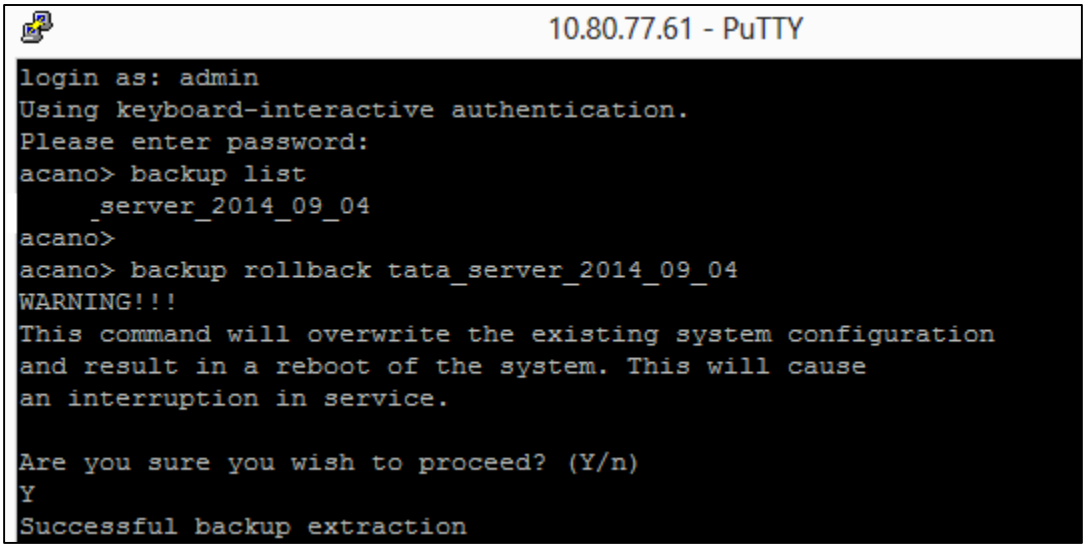
   ```
   acano> backup list      _server_2014_09_
   ```
5. Enter the following command and confirm to restore from the backup file:

   ```
   backup rollback <name>.
   ```

   This overwrites the existing configuration and reboots the Acano solution. Therefore a warning message is displayed. The confirmation is case sensitive and you must press upper case Y, otherwise the operation will be aborted.

   Note: It is not possible to create a backup from one type of deployment (Acano X series server or virtualized) and roll it back on the other type.

   A successful operation returns:




When you restore from the backup, everything is overwritten including the IP address, certificates and the license.dat file. Therefore if you are restoring onto a different server from the one that the backup was made on, you must manually copy the original license.dat file and any certificates that are not valid on the new server. Note that the license.dat file is tied to the MAC address of the server; therefore after the backup has been restored to the new server, the license from one server will be invalid on another one.

6. Establish an SFTP connection with the standby server
7. Upload the previously saved original license.dat file back on to this server
8. If necessary:
   a. Put back any certificates and private keys (if the restored versions are not valid on the standby server).
   b. Assign these certificates to their corresponding services using the following commands:

```
callbridge certs nameofkey nameofcertificate
webbridge certs nameofkey nameofcertificate
webadmin certs nameofkey nameofcertificate
xmpp certs nameofkey nameofcertificate
webbridge trust nameofcallbridgecertificate
```

   c. Restart the any service for which you changed the certificate

```
xmpp restart
callbridge restart
webbridge restart
webadmin restart
```

After the new server has fully booted up, it will be fully operation and take over the services of the original server.

## Time for Swapping Servers

If the standby server is kept powered on, typical restore times for Acano servers are 6-8 minutes (and for VM servers this is 2-4 minutes) to restore the configuration, copy the license.dat file and

restart the XMPP server. If certificate files also need to be restored, additional time may be required.